Bisimulation for quantum processes

Yuan Feng[*], Runyao Duan[†], Mingsheng Ying[‡]

Center of Quantum Computation and Intelligent Systems,
Faculty of Information Technology, University of Technology,
Sydney, NSW 2007, Australia

State Key Laboratory of Intelligent Technology and Systems,
Department of Computer Science and Technology Tsinghua University,
Beijing, China, 100084

Abstract

Quantum cryptographic systems have been commercially available, with a striking advantage over classical systems that their security and ability to detect the presence of eavesdropping are provable based on the principles of quantum mechanics. On the other hand, quantum protocol designers may commit much more faults than classical protocol designers since human intuition is much better adapted to the classical world than the quantum world. To offer formal techniques for modeling and verification of quantum protocols, several quantum extensions of process algebra have been proposed. One of the most serious issues in quantum process algebra is to discover a quantum generalization of the notion of bisimulation, which lies in a central position in process algebra, preserved by parallel composition in the presence of quantum entanglement, which has no counterpart in classical computation. Quite a few versions of bisimulation have been defined for quantum processes in the literature, but in the best case they are only proved to be preserved by parallel composition of purely quantum processes where no classical communications are involved.

Many quantum cryptographic protocols, however, employ the LOCC (Local Operations and Classical Communications) scheme, where classical communications must be explicitly specified. So, a notion of bisimulation preserved by parallel composition in the circumstance of both classical and quantum communications is crucial for process algebra approach to verification of quantum cryptographic protocols. In this paper we introduce a novel notion of bisimulation for quantum processes and prove that it is congruent with respect to various process algebra combinators including parallel composition even when both classical and quantum communications are present. We also establish some basic algebraic laws for this bisimulation. In particular, we prove uniqueness of the solutions to recursive equations of quantum processes, which provides a powerful proof technique for verifying complex quantum protocols.

1 Introduction

Quantum computing offers the potential of considerable speedup over classical computing for some important problems such as prime factoring [17] and unsorted database search [7]. However, functional quantum computers which can harness this potential in dealing with practical applications are

[*]E-mail address: yuan.feng@uts.edu.au
[†]E-mail address: runyao.duan@uts.edu.au
[‡]E-mail address: mingsheng.ying@uts.edu.au

extremely difficult to implement. On the other hand, quantum cryptography, of which the security and ability to detect the presence of eavesdropping are provable based on the principles of quantum mechanics, has been developed so rapidly that quantum cryptographic systems are already commercially available by a number of companies such as Id Quantique, Cerberis, MagiQ Technologies, SmartQuantum, and NEC.

As is well known, it is very difficult to guarantee correctness of classical communication protocols at the design stage, and some simple protocols were finally found to have fundamental flaws. Since human intuition is much worse adapted to the quantum world than the classical world, quantum protocol designers may commit much more faults than classical protocol designers, especially when more and more complicated quantum protocols can be implemented by future physical technology. With the purpose of cloning the success classical process algebras achieve in analyzing and verifying classical communication protocols and even distributed computing, various quantum process algebras have been proposed independently by several research groups. Jorrand and Lalire [10] defined a language QPAlg (Quantum Process Algebra) by extending a classical CCS-like process algebra. A branching bisimulation which identifies quantum processes associated with graphs having the same branching structure was also presented [12]. The bisimulation is, however, not congruent: it is not preserved by parallel composition. Gay and Nagarajan [6] defined a language CQP (Communicating Quantum Processes), which combines the communication primitives of pi-calculus [13] with primitives for unitary transformations and measurements. One distinctive feature of CQP is a type system which guarantees the physical realizability of quantum processes. However, no notion of equivalence between processes was presented.

Authors of the current paper proposed a model named qCCS [5] for quantum communicating systems by adding quantum input/output and quantum operation/measurement primitives to classical value-passing CCS [8, 9]. The semantics of quantum input and output was carefully designed to describe the communication of quantum systems which have been entangled with other systems. A bisimulation was defined for finite processes, and a simplified version of congruence property was proved, in which parallel composition is only permitted when the participating processes are free of quantum input, or free of quantum operations and measurement. In [19] the same authors studied a purely quantum version of qCCS where no classical data is explicitly involved, aiming at providing us a suitable framework to observe the interaction of computation and communication in quantum systems. A bisimulation was defined for this purely quantum qCCS and shown to be fully preserved by parallel composition. It is worth noting that, however, the bisimulation proposed in [19] cannot be directly extended to general qCCS where classical data as well as probabilistic behaviors are included.

In this paper, we combine the two models proposed in [5] and [19] together to involve both classical data and quantum data. This general model, which we still call qCCS for coherence, accommodates all classical process constructors (especially recursive definitions) as well as quantum primitives. As a consequence, both sequential and distributed quantum computing, quantum communication protocols, and quantum cryptographic systems can be formally modeled and rigorously analyzed in the framework of qCCS. We also design a bisimulation for processes in qCCS and an equivalence relation based on it, which turns out to be a congruence. This bisimulation has several distinctive features compared with those proposed in the literature: Firstly, it takes local quantum operations into account in a weak manner, but at the same time fits well with recursive definitions. Lalire's bisimulation cannot distinguish different operations on a quantum system which will never be output: quantum states are only compared when they are input or output. Bisimulation defined in [5] works well only for finite processes since quantum states are required to be compared after all the actions have been performed. Note that no state comparison is needed in [19] since all local quantum operations are regarded as visible actions, and the resulted bisimulation is a very strong one – it distinguishes two different sequences of local operations even when they have the same effect as a whole. Secondly, entanglement between the input/output system and the remaining systems is fully considered in our definition. Bisimulation presented in [12] totally ignores this correlation by

only considering the reduced state of the input/output system. In [5] this consideration is implicitly made by the state comparison after the processes terminating. Again, it does not work for infinite processes. Finally, but most importantly, the bisimulation presented here is preserved by parallel composition, and the equivalence derived by the bisimulation is a congruence, making them suitable for equational reasoning in verifying quantum communication and cryptographic systems. Lalire's bisimulation is not preserved by parallel composition. The bisimulation in [5] is not preserved by restriction, and whether it is preserved by parallel composition still remains open, although the positive answer is affirmed in two special cases. The bisimulation proposed in [19] is indeed a congruence. However, since no classical data is involved in that model, many important quantum communication protocols such as superdense coding and teleportation cannot be described. This restricts the scope of its application.

The paper is organized as follows: in Section 2, we review some basic notions from linear algebra and quantum mechanics. The syntax and operational semantics of qCCS are presented in Section 3. To illustrate the expressiveness of qCCS, we describe with it the well-known quantum superdense coding and teleportation protocols. We also show how to encode quantum unitary gates and measurement gates, which are two basic elements of quantum circuits, by qCCS. Section 4 defines the notion of bisimulations for configurations as well as quantum processes. Equivalence relation based on bisimularity is also defined and proved to be fully preserved by all process constructors of qCCS. The validity of examples in Section 3 is proved by using the notion of bisimilarity defined in this section. Various properties such as monoid laws, static laws, the expansion law, as well as uniqueness of solutions of process equations are also examined. We outline the main results in Section 5 and point out some problems for further study.

2 Preliminaries

For convenience of the reader, we briefly recall some basic notions from linear algebra and quantum theory which are needed in this paper. For more details, we refer to [15].

2.1 Basic linear algebra

A *Hilbert space* $\mathcal{H}$ is a complete vector space equipped with an inner product

$$\langle\cdot|\cdot\rangle : \mathcal{H}\times\mathcal{H}\to\mathbf{C}$$

such that

(1) $\langle\psi|\psi\rangle \geq 0$ for any $|\psi\rangle\in\mathcal{H}$, with equality if and only if $|\psi\rangle = 0$;

(2) $\langle\phi|\psi\rangle = \langle\psi|\phi\rangle^*$;

(3) $\langle\phi|\sum_i \lambda_i|\psi_i\rangle = \sum_i \lambda_i\langle\phi|\psi_i\rangle$,

where $\mathbf{C}$ is the set of complex numbers, and for each $\lambda\in\mathbf{C}$, λ^* stands for the complex conjugate of λ. For any vector $|\psi\rangle\in\mathcal{H}$, its length $|||\psi\rangle||$ is defined to be $\sqrt{\langle\psi|\psi\rangle}$, and it is said to be *normalized* if $|||\psi\rangle|| = 1$. Two vectors $|\psi\rangle$ and $|\phi\rangle$ are *orthogonal* if $\langle\psi|\phi\rangle = 0$. An *orthonormal basis* of a Hilbert space $\mathcal{H}$ is a basis $\{|i\rangle\}$ where each $|i\rangle$ is normalized and any pair of them are orthogonal.

Let $\mathcal{L}(\mathcal{H})$ be the set of linear operators on $\mathcal{H}$. For any $A\in\mathcal{L}(\mathcal{H})$, A is *Hermitian* if $A^\dagger = A$ where $A^\dagger$ is the adjoint operator of A such that $\langle\psi|A^\dagger|\phi\rangle = \langle\phi|A|\psi\rangle^*$ for any $|\psi\rangle, |\phi\rangle\in\mathcal{H}$. The fundamental *spectrum theorem* states that the set of all normalized eigenvectors of a Hermitian operator in $\mathcal{L}(\mathcal{H})$ contains an orthonormal basis for $\mathcal{H}$. That is, there exists a so-called spectral decomposition for each Hermitian A such that

$$A = \sum_i \lambda_i|i\rangle\langle i| = \sum_{i\in spec(A)} \lambda_i E_i$$

where the set $\{|i\rangle\}$ constitute an orthonormal basis of $\mathcal{H}$, *spec*(A) denotes the set of eigenvalues of A, and E_i is the projector to the corresponding eigenspace of λ_i. A linear operator $A \in \mathcal{L}(\mathcal{H})$ is *unitary* if $A^\dagger A = AA^\dagger = I_\mathcal{H}$ where $I_\mathcal{H}$ is the identity operator on $\mathcal{H}$. In this paper, we will use some well-known unitary operators listed as follows: the quantum control-not operator performed on two qubits with the matrix representation

$$CN = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{pmatrix}$$

under the computational basis, and the 1-qubit Hadamard operator H and Pauli operators $\sigma^0, \sigma^1, \sigma^2, \sigma^3$ defined respectively as

$$H = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}, \quad \sigma^0 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},$$

$$\sigma^1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \ \sigma^2 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \ \sigma^3 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}.$$

The *trace* of $A \in \mathcal{L}(\mathcal{H})$ is defined as $\mathrm{tr}(A) = \sum_i \langle i|A|i\rangle$ for some given orthonormal basis $\{|i\rangle\}$ of $\mathcal{H}$. It is worth noting that trace function is actually independent of the orthonormal basis selected. It is also easy to check that trace function is linear and $\mathrm{tr}(AB) = \mathrm{tr}(BA)$ for any operators $A, B \in \mathcal{L}(\mathcal{H})$.

Let $\mathcal{H}_1$ and $\mathcal{H}_2$ be two Hilbert spaces. Their *tensor product* $\mathcal{H}_1 \otimes \mathcal{H}_2$ is defined as a vector space consisting of linear combinations of the vectors $|\psi_1\psi_2\rangle = |\psi_1\rangle|\psi_2\rangle = |\psi_1\rangle \otimes |\psi_2\rangle$ with $|\psi_1\rangle \in \mathcal{H}_1$ and $|\psi_2\rangle \in \mathcal{H}_2$. Here the tensor product of two vectors is defined by a new vector such that

$$\left(\sum_i \lambda_i |\psi_i\rangle\right) \otimes \left(\sum_j \mu_j |\phi_j\rangle\right) = \sum_{i,j} \lambda_i \mu_j |\psi_i\rangle \otimes |\phi_j\rangle.$$

Then $\mathcal{H}_1 \otimes \mathcal{H}_2$ is also a Hilbert space where the inner product is defined as the following: for any $|\psi_1\rangle, |\phi_1\rangle \in \mathcal{H}_1$ and $|\psi_2\rangle, |\phi_2\rangle \in \mathcal{H}_2$,

$$\langle \psi_1 \otimes \psi_2 | \phi_1 \otimes \phi_2 \rangle = \langle \psi_1 | \phi_1 \rangle_{\mathcal{H}_1} \langle \psi_2 | \phi_2 \rangle_{\mathcal{H}_2}$$

where $\langle \cdot | \cdot \rangle_{\mathcal{H}_i}$ is the inner product of $\mathcal{H}_i$. For any $A_1 \in \mathcal{L}(\mathcal{H}_1)$ and $A_2 \in \mathcal{L}(\mathcal{H}_2)$, $A_1 \otimes A_2$ is defined as a linear operator in $\mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ such that for each $|\psi_1\rangle \in \mathcal{H}_1$ and $|\psi_2\rangle \in \mathcal{H}_2$,

$$(A_1 \otimes A_2)|\psi_1\psi_2\rangle = A_1|\psi_1\rangle \otimes A_2|\psi_2\rangle.$$

The *partial trace* of $A \in \mathcal{L}(\mathcal{H}_1 \otimes \mathcal{H}_2)$ with respected to $\mathcal{H}_1$ is defined as $\mathrm{tr}_{\mathcal{H}_1}(A) = \sum_i \langle i|A|i\rangle$ where $\{|i\rangle\}$ is an orthonormal basis of $\mathcal{H}_1$. Similarly, we can define the partial trace of A with respected to $\mathcal{H}_2$. Partial trace functions are also independent of the orthonormal basis selected.

A linear operator $\mathcal{E}$ on $\mathcal{L}(\mathcal{H})$ is *completely positive* if it maps positive operators in $\mathcal{L}(\mathcal{H})$ to positive operators in $\mathcal{L}(\mathcal{H})$, and for any auxiliary Hilbert space $\mathcal{H}'$, the trivially extended operator $\mathcal{I}_{\mathcal{H}'} \otimes \mathcal{E}$ also maps positive operators in $\mathcal{L}(\mathcal{H}' \otimes \mathcal{H})$ to positive operators in $\mathcal{L}(\mathcal{H}' \otimes \mathcal{H})$. Here $\mathcal{I}_{\mathcal{H}'}$ is the identity operator on $\mathcal{L}(\mathcal{H}')$. The elegant and powerful *Kraus representation theorem* [11] of completely positive operators states that a linear operator $\mathcal{E}$ is completely positive if and only if there are some set of operators $\{E_i\}$ with appropriate dimension such that

$$\mathcal{E}(A) = \sum_i E_i A E_i^\dagger$$

for any $A \in \mathcal{L}(\mathcal{H})$. The operators E_i are called Kraus operators of $\mathcal{E}$. A linear operator is said to be a *super-operator* if it is completely positive and trace-nonincreasing. Here an operator $\mathcal{E}$

is *trace-nonincreasing* if $\mathrm{tr}(\mathcal{E}(A)) \leq \mathrm{tr}(A)$ for any positive $A \in \mathcal{L}(\mathcal{H})$, and it is said to be *trace-preserving* if the equality always holds. Then a super-operator (resp. a trace-preserving super-operator) is a completely positive operator with its Kraus operators E_i satisfying $\sum_i E_i^\dagger E_i \leq I$ (resp. $\sum_i E_i^\dagger E_i = I$).

2.2 Basic quantum mechanics

According to von Neumann's formalism of quantum mechanics [18], an isolated physical system is associated with a Hilbert space which is called the *state space* of the system. A *pure state* of a quantum system is a normalized vector in its state space, and a *mixed state* is represented by a density operator on the state space. Here a density operator ρ on Hilbert space $\mathcal{H}$ is a positive linear operator such that $\mathrm{tr}(\rho) = 1$. Another equivalent representation of density operator is probabilistic ensemble of pure states. In particular, given an ensemble $\{(p_i, |\psi_i\rangle)\}$ where $p_i \geq 0$, $\sum_i p_i = 1$, and $|\psi_i\rangle$ are pure states, then $\rho = \sum_i p_i [|\psi_i\rangle]$ is a density operator. Here $[|\psi_i\rangle]$ denotes the abbreviation of $|\psi_i\rangle\langle\psi_i|$. Conversely, each density operator can be generated by an ensemble of pure states in this way.

It is mathematically convenient to allow the trace of a density operator to be less than 1, which makes it possible to represent both the actual state (by the normalized density operator) and the probability with which the state is reached (by its trace) in a single expression [16]. Then the set of (partial) density operators on $\mathcal{H}$ can be defined as

$$\mathcal{D}(\mathcal{H}) = \{\ \rho \in \mathcal{L}(\mathcal{H})\ :\ \rho \text{ is positive and } \mathrm{tr}(\rho) \leq 1\}.$$

The state space of a composite system (for example, a quantum system consisting of many qubits) is the tensor product of the state spaces of its components. For a mixed state ρ on $\mathcal{H}_1 \otimes \mathcal{H}_2$, partial traces of ρ have explicit physical meanings: the density operators $\mathrm{tr}_{\mathcal{H}_1}\rho$ and $\mathrm{tr}_{\mathcal{H}_2}\rho$ are exactly the reduced quantum states of ρ on the second and the first component system, respectively. Note that in general, the state of a composite system cannot be decomposed into tensor product of the reduced states on its component systems. A well-known example is the 2-qubit state

$$|\Psi\rangle = \frac{1}{\sqrt{2}}(|00\rangle + |11\rangle)$$

which appears repeatedly in our examples of this paper. This kind of state is called *entangled state*. To see the strangeness of entanglement, suppose a measurement $M = \lambda_0[|0\rangle] + \lambda_1[|1\rangle]$ is applied on the first qubit of $|\Psi\rangle$ (see the following for the definition of quantum measurements). Then after the measurement, the second qubit will definitely collapse into state $|0\rangle$ or $|1\rangle$ depending on whether the outcome λ_0 or λ_1 is observed. In other words, the measurement on the first qubit changes the state of the second qubit in some way. This is an outstanding feature of quantum mechanics which has no counterpart in classical world, and is the key to many quantum information processing tasks such as teleportation [3] and superdense coding [4].

The evolution of a closed quantum system is described by a unitary operator on its state space: if the states of the system at times t_1 and t_2 are ρ_1 and ρ_2, respectively, then $\rho_2 = U\rho_1 U^\dagger$ for some unitary operator U which depends only on t_1 and t_2. In contrast, the general dynamics which can occur in a physical system is described by a super-operator on its state space. Note that the unitary transformation $U(\rho) = U\rho U^\dagger$ is a trace-preserving super-operator.

A quantum *measurement* is described by a collection $\{M_m\}$ of measurement operators, where the indices m refer to the measurement outcomes. It is required that the measurement operators satisfy the completeness equation $\sum_m M_m^\dagger M_m = I_{\mathcal{H}}$. If the system is in state ρ, then the probability that measurement result m occurs is given by

$$p(m) = \mathrm{tr}(M_m^\dagger M_m \rho),$$

and the state of the post-measurement system is $M_m \rho M_m^\dagger / p(m)$.

A particular case of measurement is *projective measurement* which is usually represented by a Hermitian operator. Let M be a Hermitian operator and

$$M = \sum_{m \in spec(M)} m E_m$$

its spectral decomposition. Obviously, the projectors $\{E_m : m \in spec(M)\}$ form a quantum measurement. If the state of a quantum system is ρ, then the probability that result m occurs when measuring M on the system is $p(m) = \mathrm{tr}(E_m \rho)$, and the post-measurement state of the system is $E_m \rho E_m / p(m)$. Note that for each outcome m, the map

$$\mathcal{E}_m(\rho) = E_m \rho E_m$$

is again a super-operator by Kraus Theorem; it is not trace-preserving in general.

3 Basic definitions of qCCS

In this section, we give the basic definitions of qCCS, which is a combination of those proposed in [5] and [19], involving classical data as well as quantum data, all classical process constructors (especially the recursive definition) as well as quantum primitives. The reader is referred to [5] and [19] for further examples and explanations of the language.

3.1 Syntax

For simplicity, only two types of data are considered in qCCS: real numbers Real for classical data and qubits Qbt for quantum data. Let $cVar$, ranged over by $x, y, \ldots$, be the set of classical variables and $qVar$, ranged over by $q, r, \ldots$, the set of quantum variables. It is assumed that $cVar$ and $qVar$ are both countably infinite. Let Exp, ranged over by e, be the set of expressions with the value domain Real. Let $cChan$ be the set of classical channel names, ranged over by $c, d, \ldots$, and $qChan$ the set of quantum channel names, ranged over by $\mathsf{c}, \mathsf{d}, \ldots$. Let $Chan = cChan \cup qChan$. A relabeling function f is a one to one function from $Chan$ to $Chan$ such that $f(cChan) \subseteq cChan$ and $f(qChan) \subseteq qChan$.

We often abbreviate the indexed set $\{q_1, \ldots, q_n\}$ to $\widetilde{q}$ when $q_1, \ldots, q_n$ are distinct quantum variables and the dimension n is understood. Sometimes we also use $\widetilde{q}$ to denote the string $q_1 \ldots q_n$. We assume a set of process constant schemes, ranged over by $A, B, \ldots$. Assigned to each process constant scheme A there is a non-negative integer $ar(A)$. If $\widetilde{q}$ is a tuple of distinct quantum variables with $|\widetilde{q}| = ar(A)$, then $A(\widetilde{q})$ is called a process constant.

Based on these notations, we now propose the syntax of qCCS as follows.

Definition 3.1 (Quantum process) The set of quantum processes $qProc$ and the free quantum variable function $qv : qProc \to 2^{qVar}$ are defined inductively by the following formation rules:

(1) $\mathbf{nil} \in qProc$, and $qv(\mathbf{nil}) = \emptyset$;

(2) $A(\widetilde{q}) \in qProc$, and $qv(A(\widetilde{q})) = \widetilde{q}$;

(3) $\tau.P \in qProc$, and $qv(\tau.P) = qv(P)$;

(4) $c?x.P \in qProc$, and $qv(c?x.P) = qv(P)$;

(5) $c!e.P \in qProc$, and $qv(c!e.P) = qv(P)$;

(6) $\mathsf{c}?q.P \in qProc$, and $qv(\mathsf{c}?q.P) = qv(P) - \{q\}$;

(7) If $q \notin qv(P)$ then $\mathsf{c}!q.P \in qProc$, and $qv(\mathsf{c}!q.P) = qv(P) \cup \{q\}$;

(8) $\mathcal{E}[\widetilde{q}].P \in qProc$, and $qv(\mathcal{E}[\widetilde{q}].P) = qv(P) \cup \widetilde{q}$;

(9) $M[\widetilde{q}; x].P \in qProc$, and $qv(M[\widetilde{q}; x].P) = qv(P) \cup \widetilde{q}$;

(10) $P + Q \in qProc$, and $qv(P + Q) = qv(P) \cup qv(Q)$;

(11) If $qv(P) \cap qv(Q) = \emptyset$ then $P \| Q \in qProc$, and $qv(P \| Q) = qv(P) \cup qv(Q)$;

(12) $P[f] \in qProc$, and $qv(P[f]) = qv(P)$;

(13) $P \backslash L \in qProc$, and $qv(P \backslash L) = qv(P)$;

(14) **if** b **then** $P \in qProc$, and $qv($**if** b **then** $P) = qv(P)$,

where $P, Q \in qProc$, $c \in cChan$, $x \in cVar$, $\mathsf{c} \in qChan$, $q \in qVar$, $\widetilde{q} \subseteq qVar$, $e \in Exp$, τ is the silent action, $A(\widetilde{q})$ is a process constant, f is a relabeling function, $L \subseteq Chan$, b is a boolean-valued expression, $\mathcal{E}$ and M are respectively a trace-preserving super-operator and a Hermitian operator applying on the Hilbert space associated with the systems $\widetilde{q}$. Furthermore, for each process constant $A(\widetilde{q})$, there is a defining equation

$$A(\widetilde{q}) \stackrel{def}{=} P$$

where $P \in qProc$ with $qv(P) \subseteq \widetilde{q}$. When $\widetilde{q} = \emptyset$, we simply denote $A(\widetilde{q})$ as A.

The notion of free classical variables in quantum processes can be defined in the usual way with a unique modification that quantum measurement $M[\widetilde{q}; x]$ has binding power on x. A quantum process P is closed if it contains no free classical variables, *i.e.*, $fv(P) = \emptyset$.

3.2 Operational semantics

To present the operational semantics of qCCS, some further notations are necessary. For each quantum variable $q \in qVar$, we assume a 2-dimensional Hilbert space $\mathcal{H}_q$ to be the state space of the q-system. For any $S \subseteq qVar$, we denote

$$\mathcal{H}_S = \bigotimes_{q \in S} \mathcal{H}_q.$$

In particular, $\mathcal{H} = \mathcal{H}_{qVar}$ is the state space of the whole environment consisting of all the quantum variables. Note that $\mathcal{H}$ is a countably infinite-dimensional Hilbert space.

Suppose P is a closed quantum process. A pair of the form $\langle P, \rho \rangle$ is called a configuration, where $\rho \in \mathcal{D}(\mathcal{H})$ is a density operator on $\mathcal{H}$. The set of configurations is denoted by Con. We sometimes let $\mathcal{C}, \mathcal{D}, \ldots$ range over Con to ease notations.

Let $D(Con)$ be the set of finite-support probability distributions over Con; that is,

$$D(Con) = \{\mu : Con \to [0,1] \mid \mu(\mathcal{C}) > 0 \text{ for finitely many } \mathcal{C}, \text{ and } \sum_{\mu(\mathcal{C})>0} \mu(\mathcal{C}) = 1\}.$$

For any $\mu \in D(Con)$, we denote by $supp(\mu)$ the support set of μ, *i.e.*, the set of configurations $\mathcal{C}$ such that $\mu(\mathcal{C}) > 0$. When μ is a simple distribution such that $supp(\mu) = \{\mathcal{C}\}$ for some $\mathcal{C}$, we abuse the notation slightly to denote μ by $\mathcal{C}$. Sometimes we find it convenient to denote a distribution μ

by an explicit form $\mu = \boxplus_{i\in I} p_i \bullet \mathcal{C}_i$ (or $\mu = \boxplus p_i \bullet \mathcal{C}_i$ when the index set I is understood) where $\mathcal{C}_i$ are distinct configurations, $supp(\mu) = \{\mathcal{C}_i \ : \ i \in I\}$, and $\mu(\mathcal{C}_i) = p_i$ for each $i \in I$.

Given $\mu_1, \ldots, \mu_n \in D(Con)$ and $p_1, \ldots, p_n \in [0,1]$, $\sum_i p_i = 1$, we define the combined distribution, denoted by $\sum_{i=1}^n p_i\mu_i$, to be a new distribution μ such that $supp(\mu) = \bigcup_i supp(\mu_i)$, and for any $\mathcal{D} \in supp(\mu)$, $\mu(\mathcal{D}) = \sum_i p_i\mu_i(\mathcal{D})$.

It is worth pointing out the difference between the two notations $\boxplus_{i\in I} p_i \bullet \mathcal{C}_i$ and $\sum_{i\in I} p_i\mathcal{C}_i$: the former is the explicit form of a distribution, so it is required that $p_i > 0$ for each $i \in I$, and $\mathcal{C}_i \neq \mathcal{C}_j$ for $i \neq j$; while the latter is a combined distribution of the simple distributions $\mathcal{C}_i$ with the probability weights p_i, so p_i may be zero for some $i \in I$, and $\mathcal{C}_i$ are not necessarily distinct.

Let $\mu = \boxplus_{i\in I} p_i \bullet \langle P_i, \rho_i\rangle$. We denote by $qv(\mu)$ the free variables of μ; that is, $qv(\mu) = \bigcup_{i\in I} qv(P_i)$. We write $\mathrm{tr}(\mu) = \sum_{i\in I} p_i \mathrm{tr}(\rho_i)$, and $\mathcal{E}(\mu) = \boxplus_{i\in I} p_i \bullet \langle P_i, \mathcal{E}(\rho_i)\rangle$ when $\mathcal{E}$ is a super-operator.

Let

$$\begin{array}{rcl} Act & = & \{\tau\} \cup \{c?v, c!v \mid c \in cChan, v \in \mathsf{Real}\} \cup \\ & & \{\mathsf{c}?r, \mathsf{c}!r \mid \mathsf{c} \in qChan, r \in qVar\}. \end{array}$$

For each $\alpha \in Act$, we define the bound quantum variable $bv(\alpha)$ of α as $bv(\mathsf{c}?r) = \{r\}$ and $bv(\alpha) = \emptyset$ if α is not a quantum input. The channel name used in action α is denoted by $cn(\alpha)$; that is, $cn(c?v) = cn(c!v) = \{c\}$, $cn(\mathsf{c}?r) = cn(\mathsf{c}!r) = \{\mathsf{c}\}$, and $cn(\tau) = \emptyset$.

The semantics of qCCS is given by the probabilistic labeled transition system $(Con, Act, \longrightarrow)$, where $\longrightarrow \subseteq Con \times Act \times D(Con)$ is the smallest relation satisfying the rules defined in Figs. 1 and 2 (For brevity, we write $\langle P, \rho\rangle \xrightarrow{\alpha} \mu$ instead of $(\langle P, \rho\rangle, \alpha, \mu) \in \longrightarrow$. The symmetric forms for Rules **Inp-Int**, **Oth-Int**, and **Sum** are omitted).

The transition relation $\longrightarrow$ can be lifted to $D(Con) \times Act \times D(Con)$ by writing $\mu \xrightarrow{\alpha} \nu$ if for any $\mathcal{C} \in supp(\mu)$, $\mathcal{C} \xrightarrow{\alpha} \nu_{\mathcal{C}}$ for some $\nu_{\mathcal{C}}$, and $\nu = \sum_{\mathcal{C}\in supp(\mu)} \mu(\mathcal{C})\nu_{\mathcal{C}}$.

For any $S \subseteq qVar$ we denote by $\overline{S}$ the complement set of S in $qVar$. The following lemmas can be easily observed from the inference rules defined above.

Lemma 3.2 *If $\langle P, \rho\rangle \xrightarrow{\alpha} \mu$, then $qv(\mu) \subseteq qv(P) \cup \{bv(\alpha)\}$.*

Proof. By induction on the inference rules. □

Lemma 3.3 *If $\langle P, \rho\rangle \xrightarrow{\alpha} \mu$, then*

(1) $\mathrm{tr}(\rho) = \mathrm{tr}(\mu)$*;*

(2) there exist a set of super-operators $\{\mathcal{E}_i : i \in I\}$ acting on $\mathcal{H}_{qv(P)}$ such that for any $\sigma \in \mathcal{D}(\mathcal{H})$,

$$\langle P, \sigma\rangle \xrightarrow{\alpha} \boxplus_{i\in I} q_i^\sigma \bullet \langle P_i, \mathcal{E}_i(\sigma)/q_i^\sigma\rangle$$

where $q_i^\sigma = \mathrm{tr}(\mathcal{E}_i(\sigma))/\mathrm{tr}(\sigma)$;

(3) for any super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{qv(P)}}$,

$$\langle P, \mathcal{E}(\rho)\rangle \xrightarrow{\alpha} \mathcal{E}(\mu).$$

Proof. By induction on the inference rules. □

$$\textbf{Tau}: \quad \frac{}{\langle \tau.P, \rho\rangle \xrightarrow{\tau} \langle P, \rho\rangle}$$

$$\textbf{C-Inp}: \quad \frac{}{\langle c?x.P, \rho\rangle \xrightarrow{c?v} \langle P\{v/x\}, \rho\rangle}, \quad v \in \mathsf{Real}$$

$$\textbf{C-Outp}: \quad \frac{}{\langle c!e.P, \rho\rangle \xrightarrow{c!v} \langle P, \rho\rangle}, \quad v = [\![e]\!]$$

$$\textbf{C-Com}: \quad \frac{\langle P_1, \rho\rangle \xrightarrow{c?v} \langle P_1', \rho\rangle, \quad \langle P_2, \rho\rangle \xrightarrow{c!v} \langle P_2', \rho\rangle}{\langle P_1 \| P_2, \rho\rangle \xrightarrow{\tau} \langle P_1' \| P_2', \rho\rangle}$$

$$\textbf{Q-Inp}: \quad \frac{}{\langle \mathsf{c}?q.P, \rho\rangle \xrightarrow{\mathsf{c}?r} \langle P\{r/q\}, \rho\rangle}, \quad r \notin qv(\mathsf{c}?q.P)$$

$$\textbf{Q-Outp}: \quad \frac{}{\langle \mathsf{c}!q.P, \rho\rangle \xrightarrow{\mathsf{c}!q} \langle P, \rho\rangle}$$

$$\textbf{Q-Com}: \quad \frac{\langle P_1, \rho\rangle \xrightarrow{\mathsf{c}?r} \langle P_1', \rho\rangle, \quad \langle P_2, \rho\rangle \xrightarrow{\mathsf{c}!r} \langle P_2', \rho\rangle}{\langle P_1 \| P_2, \rho\rangle \xrightarrow{\tau} \langle P_1' \| P_2', \rho\rangle}$$

$$\textbf{Oper}: \quad \frac{}{\langle \mathcal{E}[\widetilde{r}].P, \rho\rangle \xrightarrow{\tau} \langle P, \mathcal{E}_{\widetilde{r}}(\rho)\rangle}$$

$$\textbf{Meas}: \quad \frac{}{\langle M[\widetilde{r}; x].P, \rho\rangle \xrightarrow{\tau} \sum_{i\in I} p_i \langle P\{\lambda_i/x\}, E^i_{\widetilde{r}}\rho E^i_{\widetilde{r}}/p_i\rangle}$$

where M has the spectrum decomposition
$M = \sum_{i\in I} \lambda_i E^i$ and $p_i = \mathrm{tr}(E^i_{\widetilde{r}}\rho)/\mathrm{tr}(\rho)$

Figure 1: Inference rules for qCCS (Part 1)

3.3 Examples

To illustrate the expressiveness of qCCS, we give some examples.

Example 3.4 Superdense coding [4] is a quantum protocol using which two bits of classical information can be faithfully transmitted by sending only one qubit, provided that a maximally entangled state is shared *a priori* between the sender and the receiver. The protocol goes as follows. Let $|\Psi\rangle = (|00\rangle + |11\rangle)/\sqrt{2}$ be the entangled state shared between the sender Alice and the receiver Bob. Alice applies a Pauli operator on her qubit of $|\Psi\rangle$ according to which information among the four possibilities she wishes to transmit, and sends her qubit to Bob. With the two qubits in hand, Bob performs a perfect discrimination among the possible states (they are actually the four Bell states $\{\sigma^i \otimes I|\Psi\rangle : i = 0, 1, 2, 3\}$ where σ^i are defined in Section 2) and retrieves the information Alice has sent.

We now show how to describe the protocol of superdense coding with qCCS. Let M be a 2-qubit measurement such that $M = \sum_{i=0}^{3} i|\tilde{i}\rangle\langle\tilde{i}|$, where $\tilde{i}$ is the binary expansion of i. Let CN be the controlled-not operator and H Hadamard operator. Then the quantum processes participated in

$$\textbf{Inp-Int}: \quad \frac{\langle P_1, \rho\rangle \xrightarrow{\mathsf{c}?r} \langle P_1', \rho\rangle,\ r \notin qv(P_2)}{\langle P_1 \| P_2, \rho\rangle \xrightarrow{\mathsf{c}?r} \langle P_1' \| P_2, \rho\rangle}$$

$$\textbf{Oth-Int}: \quad \frac{\langle P_1, \rho\rangle \xrightarrow{\alpha} \boxplus_{i\in I} p_i \bullet \langle P_i', \rho_i\rangle,\ \alpha \neq \mathsf{c}?r}{\langle P_1 \| P_2, \rho\rangle \xrightarrow{\alpha} \boxplus_{i\in I} p_i \bullet \langle P_i' \| P_2, \rho_i\rangle}$$

$$\textbf{Sum}: \quad \frac{\langle P, \rho\rangle \xrightarrow{\alpha} \mu}{\langle P + Q, \rho\rangle \xrightarrow{\alpha} \mu}$$

$$\textbf{Rel}: \quad \frac{\langle P, \rho\rangle \xrightarrow{\alpha} \boxplus p_i \bullet \langle P_i, \rho_i\rangle}{\langle P[f], \rho\rangle \xrightarrow{f(\alpha)} \boxplus p_i \bullet \langle P_i[f], \rho_i\rangle}$$

$$\textbf{Res}: \quad \frac{\langle P, \rho\rangle \xrightarrow{\alpha} \boxplus p_i \bullet \langle P_i, \rho_i\rangle,\ cn(\alpha) \notin L}{\langle P \backslash L, \rho\rangle \xrightarrow{\alpha} \boxplus p_i \bullet \langle P_i \backslash L, \rho_i\rangle}$$

$$\textbf{Cho}: \quad \frac{\langle P, \rho\rangle \xrightarrow{\alpha} \mu,\ [\![b]\!] = \text{true}}{\langle \textbf{if } b \textbf{ then } P, \rho\rangle \xrightarrow{\alpha} \mu}$$

$$\textbf{Def}: \quad \frac{\langle P\{\widetilde{r}/\widetilde{q}\}, \rho\rangle \xrightarrow{\alpha} \mu,\ A(\widetilde{q}) \stackrel{def}{=} P}{\langle A(\widetilde{r}), \rho\rangle \xrightarrow{\alpha} \mu}$$

Figure 2: Inference rules for qCCS (Part 2)

superdense coding protocol can be defined as follows:

$$\begin{aligned}
Alice_s &= c?x. \sum_{0\leq i\leq 3} \left(\textbf{if } x = i \textbf{ then } \sigma^i[q_1].\mathsf{e}!q_1.\textbf{nil}\right), \\
Bob_s &= \mathsf{e}?q_1.CN[q_1, q_2].H[q_1].M[q_1, q_2; x].d!x.\textbf{nil}, \\
Sdc &= (Alice_s \| Bob_s) \backslash \{\mathsf{e}\}.
\end{aligned}$$

For any $\rho \in \mathcal{D}(\mathcal{H}_{\overline{\{q_1,q_2\}}})$ and $v \in \{0,1,2,3\}$, we have the transitions

$$
\begin{aligned}
& \langle Sdc, [|\Psi\rangle]_{q_1,q_2} \otimes \rho\rangle \\
\xrightarrow{c?v} \quad & \langle \left(\left(\sum_{0\le i\le 3} (\textbf{if } v = i \textbf{ then } \sigma^i[q_1].\mathsf{e}!q_1.\textbf{nil}) \right) \| Bob_s \right) \backslash \{\mathsf{e}\}, \\
& \qquad [|\Psi\rangle]_{q_1,q_2} \otimes \rho\rangle \\
\xrightarrow{\tau} \quad & \langle (\mathsf{e}!q_1.\textbf{nil} \| Bob_s)\backslash\{\mathsf{e}\}, \sigma^v_{q_1}([|\Psi\rangle]) \otimes \rho\rangle \\
\xrightarrow{\tau} \quad & \langle (\textbf{nil} \| CN[q_1,q_2].H[q_1].M[q_1,q_2;x].d!x.\textbf{nil})\backslash\{\mathsf{e}\}, \\
& \qquad \sigma^v_{q_1}([|\Psi\rangle]) \otimes \rho\rangle \\
\xrightarrow{\tau} \quad & \langle (\textbf{nil} \| H[q_1].M[q_1,q_2;x].d!x.\textbf{nil})\backslash\{\mathsf{e}\}, \\
& \qquad CN_{q_1,q_2}(\sigma^v_{q_1}([|\Psi\rangle])) \otimes \rho\rangle \\
\xrightarrow{\tau} \quad & \langle (\textbf{nil} \| M[q_1,q_2;x].d!x.\textbf{nil})\backslash\{\mathsf{e}\}, [|\widetilde{v}\rangle]_{q_1,q_2} \otimes \rho\rangle \qquad (1) \\
\xrightarrow{\tau} \quad & \langle (\textbf{nil} \| d!v.\textbf{nil})\backslash\{\mathsf{e}\}, [|\widetilde{v}\rangle]_{q_1,q_2} \otimes \rho\rangle \\
\xrightarrow{d!v} \quad & \langle (\textbf{nil} \| \textbf{nil})\backslash\{\mathsf{e}\}, [|\widetilde{v}\rangle]_{q_1,q_2} \otimes \rho\rangle.
\end{aligned}
$$

Here Eq.(1) is calculated as follows:

$$
H_{q_1}(CN_{q_1,q_2}(\sigma^v_{q_1}([|\Psi\rangle]))) =
$$

$$
\begin{cases}
H_{q_1}(CN_{q_1,q_2}([\frac{|00\rangle+|11\rangle}{\sqrt{2}}])) = [|00\rangle], \text{ if } v = 0 \\
H_{q_1}(CN_{q_1,q_2}([\frac{|10\rangle+|01\rangle}{\sqrt{2}}])) = [|01\rangle], \text{ if } v = 1 \\
H_{q_1}(CN_{q_1,q_2}([\frac{|00\rangle-|11\rangle}{\sqrt{2}}])) = [|10\rangle], \text{ if } v = 2 \\
H_{q_1}(CN_{q_1,q_2}([\frac{|01\rangle-|10\rangle}{\sqrt{2}}])) = [|11\rangle], \text{ if } v = 3.
\end{cases}
$$

Example 3.5 Quantum teleportation [3] is one of the most important protocols in quantum information theory which can make use of a maximally entangled state shared between the sender and the receiver to teleport an unknown quantum state by sending only classical information. It serves as a key ingredient in many other communication protocols. The protocol goes as follows. Let $|\Psi\rangle_{q_1,q_2}$ be the entanglement state shared between the sender Alice and the receiver Bob, with Alice holding q_1 and Bob holding q_2. Let q be the quantum system whose state Alice want to transmit to Bob. Alice first applies a quantum control-not operations on q and q_1, with q the control qubit and q_1 the target, followed by a Hadamard operator H on q. She then measures q and q_1 according to the computational basis, and sends the measurement outcome to Bob. Upon receiving the classical bits from Alice, Bob applies a corresponding Pauli operator on his qubit q_2 to recover the original state of q.

Let M, CN, H, and $\sigma^i,\ i = 0, \ldots, 3$ be as defined in Example 3.4. Then the quantum processes participated in teleportation protocol can be defined as follows:

$$
\begin{aligned}
Alice_t &= \mathsf{c}?q.CN[q,q_1].H[q].M[q,q_1;x].e!x.\textbf{nil}, \\
Bob_t &= e?x. \sum_{0\le i\le 3} (\textbf{if } x = i \textbf{ then } \sigma^i[q_2].\mathsf{d}!q_2.\textbf{nil}), \\
Tel &= (Alice_t \| Bob_t)\backslash\{e\},
\end{aligned}
$$

For any $\rho \in \mathcal{D}(\mathcal{H}_{\overline{\{q_1,q_2\}}})$, we have

$$
\begin{aligned}
& \langle Tel, [|\Psi\rangle]_{q_1,q_2} \otimes \rho \rangle \\
\xrightarrow{\mathsf{c}?r} \quad & \langle (CN[r,q_1].H[r].M[r,q_1;x].c!x.\mathbf{nil} \| Bob_t)\backslash\{e\}, \\
& \qquad\qquad [|\Psi\rangle]_{q_1,q_2} \otimes \rho \rangle \\
\xrightarrow{\tau} \quad & \langle (H[r].M[r,q_1;x].c!x.\mathbf{nil} \| Bob_t)\backslash\{e\}, \\
& \qquad\qquad CN_{r,q_1}([|\Psi\rangle]_{q_1,q_2} \otimes \rho) \rangle \\
\xrightarrow{\tau} \quad & \langle (M[r,q_1;x].c!x.\mathbf{nil} \| Bob_t)\backslash\{e\}, \\
& \qquad\qquad \sum_{0 \le j \le 3} \frac{1}{4} [|\widetilde{j}\rangle]_{r,q_1} \otimes \sigma^j_{q_2}(\rho) \rangle \qquad (2) \\
\xrightarrow{\tau} \quad & 1/4 \bullet \langle (c!0.\mathbf{nil} \| Bob_t)\backslash\{e\}, [|00\rangle]_{r,q_1} \otimes \rho \rangle \\
& \boxplus 1/4 \bullet \langle (c!1.\mathbf{nil} \| Bob_t)\backslash\{e\}, [|01\rangle]_{r,q_1} \otimes \sigma^1_{q_2}(\rho) \rangle \\
& \boxplus 1/4 \bullet \langle (c!2.\mathbf{nil} \| Bob_t)\backslash\{e\}, [|10\rangle]_{r,q_1} \otimes \sigma^2_{q_2}(\rho) \rangle \\
& \boxplus 1/4 \bullet \langle (c!3.\mathbf{nil} \| Bob_t)\backslash\{e\}, [|11\rangle]_{r,q_1} \otimes \sigma^3_{q_2}(\rho) \rangle,
\end{aligned}
$$

and for $0 \le j \le 3$,

$$
\begin{aligned}
& \langle (c!j.\mathbf{nil} \| Bob_t)\backslash\{e\}, [|\widetilde{j}\rangle]_{r,q_1} \otimes \sigma^j_{q_2}(\rho) \rangle \\
\xrightarrow{\tau} \quad & \langle (\mathbf{nil} \| \sum_{0 \le i \le 3} (\mathbf{if}\ j = i\ \mathbf{then}\ \sigma^i[q_2].\mathsf{d}!q_2.\mathbf{nil}))\backslash\{e\}, \\
& \qquad\qquad [|\widetilde{j}\rangle]_{r,q_1} \otimes \sigma^j_{q_2}(\rho) \rangle \\
\xrightarrow{\tau} \quad & \langle (\mathbf{nil} \| \mathsf{d}!q_2.\mathbf{nil})\backslash\{e\}, [|\widetilde{j}\rangle]_{r,q_1} \otimes \rho \rangle \\
\xrightarrow{\mathsf{d}!q_2} \quad & \langle (\mathbf{nil} \| \mathbf{nil})\backslash\{e\}, [|\widetilde{j}\rangle]_{r,q_1} \otimes \rho \rangle.
\end{aligned}
$$

Here Eq.(2) is calculated as follows. Notice that any $\rho \in \mathcal{D}(\mathcal{H}_{\overline{\{q_1,q_2\}}})$ can be decomposed as $\rho = \sum_{0 \le i \le 3} \gamma_i [|\psi_i\rangle]_r \otimes \rho_i$ where $|\psi_0\rangle = |0\rangle, |\psi_1\rangle = |1\rangle, |\psi_2\rangle = |+\rangle = (|0\rangle + |1\rangle)/\sqrt{2}$, and $|\psi_3\rangle = |-\rangle = (|0\rangle - |1\rangle)/\sqrt{2}$. Then it is easy to derive that

$$
\begin{aligned}
& H_r(CN_{r,q_1}([|\Psi\rangle]_{q_1,q_2} \otimes \rho)) \\
= \quad & \frac{\gamma_0}{4} [|000\rangle + |011\rangle + |100\rangle + |111\rangle]_{r,q_1,q_2} \otimes \rho_1 \\
& + \frac{\gamma_1}{4} [|001\rangle + |010\rangle - |101\rangle - |110\rangle]_{r,q_1,q_2} \otimes \rho_2 \\
& + \frac{\gamma_2}{4} [|00+\rangle + |01+\rangle + |10-\rangle - |11-\rangle]_{r,q_1,q_2} \otimes \rho_3 \\
& + \frac{\gamma_3}{4} [|00-\rangle - |01-\rangle + |10+\rangle + |11+\rangle]_{r,q_1,q_2} \otimes \rho_4 \\
\\
= \quad & \frac{1}{4} [|00\rangle]_{r,q_1} \otimes \rho + \frac{1}{4} [|01\rangle]_{r,q_1} \otimes \sigma^1_{q_2}(\rho) \\
& + \frac{1}{4} [|10\rangle]_{r,q_1} \otimes \sigma^2_{q_2}(\rho) + \frac{1}{4} [|11\rangle]_{r,q_1} \otimes \sigma^3_{q_2}(\rho).
\end{aligned}
$$

Example 3.6 (Encode quantum circuits with qCCS) Quantum circuits consist of two different types of gates: unitary gates and quantum measurements. We now show how to encode them using qCCS. To ease the notations, we allow quantum channels to input and output multiple qubits. We write the quantum channel c as c^n if n qubits can be communicated through c simultaneously. In other words, the quantum capacity of c^n is n qubits.

- Unitary gate. Suppose U is a unitary operator acting on n qubits. Then the unitary gate which implements U can be defined as a process constant $\mathcal{U}(U)$, $qv(\mathcal{U}(U)) = \emptyset$, with the defining equation
$$\mathcal{U}(U) \stackrel{def}{=} \mathsf{c}^n?\widetilde{q}.U[\widetilde{q}].\mathsf{d}^n!\widetilde{q}.\mathcal{U}(U).$$
We denote $ar(\mathcal{U}(U)) = n$.

- Measurement gate. Suppose M is a quantum measurement acting on n qubits. Then the measurement gate which implements M can be defined as
$$\mathcal{M}(M) \stackrel{def}{=} \mathsf{c}^n?\widetilde{q}.M[\widetilde{q};x].e!x.\mathsf{d}^n!\widetilde{q}.\mathcal{M}(M).$$
We denote $ar(\mathcal{M}(M)) = n$.

For any $\rho \in \mathcal{D}(\mathcal{H})$, we have

$$\begin{array}{rcl} \langle \mathcal{U}(U), \rho \rangle & \xrightarrow{\mathsf{c}^n?\widetilde{r}} & \langle U[\widetilde{r}].\mathsf{d}^n!\widetilde{r}.\mathcal{U}(U), \rho \rangle \\ & \xrightarrow{\tau} & \langle \mathsf{d}^n!\widetilde{r}.\mathcal{U}(U), U_{\widetilde{r}}\rho U_{\widetilde{r}}^\dagger \rangle \\ & \xrightarrow{\mathsf{d}^n!\widetilde{r}} & \langle \mathcal{U}(U), U_{\widetilde{r}}\rho U_{\widetilde{r}}^\dagger \rangle \end{array}$$

and

$$\begin{array}{rcl} \langle \mathcal{M}(M), \rho \rangle & \xrightarrow{\mathsf{c}^n?\widetilde{r}} & \langle M[\widetilde{r};x].e!x.\mathsf{d}^n!\widetilde{r}.\mathcal{M}(M), \rho \rangle \\ & \xrightarrow{\tau} & \boxplus_{i\in I} p_i \bullet \langle e!\lambda_i.\mathsf{d}^n!\widetilde{r}.\mathcal{M}(M), E^i_{\widetilde{r}}\rho E^i_{\widetilde{r}}/p_i \rangle \end{array}$$

where $M = \sum_{i\in I} \lambda_i E^i$ and $p_i = \mathrm{tr}(E^i_{\widetilde{r}}\rho)/\mathrm{tr}(\rho)$. Now for each $i \in I$,

$$\begin{array}{rl} & \langle e!\lambda_i.\mathsf{d}^n!\widetilde{r}.\mathcal{M}(M), E^i_{\widetilde{r}}\rho E^i_{\widetilde{r}}/p_i \rangle \\ \xrightarrow{e!\lambda_i} & \langle \mathsf{d}^n!\widetilde{r}.\mathcal{M}(M), E^i_{\widetilde{r}}\rho E^i_{\widetilde{r}}/p_i \rangle \\ \xrightarrow{\mathsf{d}^n!\widetilde{r}} & \langle \mathcal{M}(M), E^i_{\widetilde{r}}\rho E^i_{\widetilde{r}}/p_i \rangle. \end{array}$$

Suppose $\mathcal{G}_1$ and $\mathcal{G}_2$ are two (unitary or measurement) gates with $ar(\mathcal{G}_1) = ar(\mathcal{G}_2) = n$. The sequential composition of $\mathcal{G}_1$ and $\mathcal{G}_2$ can be defined as

$$\begin{array}{rcl} \mathcal{G}_1 \circ \mathcal{G}_2 & \stackrel{def}{=} & (L_s \| \mathcal{G}_1[\mathsf{e}^n/\mathsf{c}^n, \mathsf{f}^n/\mathsf{d}^n] \| \mathcal{G}_2[\mathsf{f}^n/\mathsf{c}^n, \mathsf{g}^n/\mathsf{d}^n] \| R_s) \backslash \\ & & \{c, \mathsf{e}^n, \mathsf{f}^n, \mathsf{g}^n\} \end{array}$$

where $L_s \stackrel{def}{=} \mathsf{c}^n?\widetilde{q}.\mathsf{e}^n!\widetilde{q}.c?x.L_s$ and $R_s \stackrel{def}{=} \mathsf{g}^n?\widetilde{q}.\mathsf{d}^n!\widetilde{q}.c!0.R_s$.

If $ar(\mathcal{G}_1) = m$ and $ar(\mathcal{G}_2) = n$, then the parallel composition of $\mathcal{G}_1$ and $\mathcal{G}_2$ is defined as

$$\begin{array}{rcl} \mathcal{G}_1 \otimes \mathcal{G}_2 & \stackrel{def}{=} & (L_p \| \mathcal{G}_1[\mathsf{e}_1^m/\mathsf{c}^m, \mathsf{f}_1^m/\mathsf{d}^m] \| \mathcal{G}_2[\mathsf{e}_2^n/\mathsf{c}^n, \mathsf{f}_2^n/\mathsf{d}^n] \\ & & \| R_p) \backslash \{c, \mathsf{e}_1^m, \mathsf{f}_1^m, \mathsf{e}_2^n, \mathsf{f}_2^n\} \end{array}$$

where $L_p \stackrel{def}{=} \mathsf{c}^{m+n}?\widetilde{q}.\mathsf{e}_1^m!l(\widetilde{q}).\mathsf{e}_2^n!r(\widetilde{q}).c?x.L_p$,

$$R_p \stackrel{def}{=} \mathsf{f}_1^m?\widetilde{r_1}.\mathsf{f}_2^n?\widetilde{r_2}.\mathsf{d}^{m+n}!(\widetilde{r_1}\widetilde{r_2}).c!0.R_p,$$

$l(\widetilde{q})$ denotes the prefix of $\widetilde{q}$ with length m while $r(\widetilde{q})$ the postfix of $\widetilde{q}$ with length n, and $\widetilde{r_1}\widetilde{r_2}$ is the concatenation of $\widetilde{r_1}$ and $\widetilde{r_2}$.

4 (Weak) Bisimulation between quantum processes

To present the notion of bisimulation which abstracts the internal actions caused by local quantum operations and (classical or quantum) communications, we first extend the transition relation defined in Section 3.

Definition 4.1 We define the relation $\Longrightarrow \subseteq Con \times D(Con)$ as the smallest relation satisfying the following conditions:

(1) $\mathcal{C} \Longrightarrow \mathcal{C}$;

(2) if $\mathcal{C} \stackrel{\tau}{\longrightarrow} \boxplus_{i\in I} p_i \bullet \mathcal{C}_i$ and $\mathcal{C}_i \Longrightarrow \mu_i$ for each $i \in I$, then $\mathcal{C} \Longrightarrow \sum p_i \mu_i$.

Similar to $\longrightarrow$, we can also lift $\Longrightarrow$ to $D(Con) \times D(Con)$ by writing $\mu \Longrightarrow \nu$ if for each $\mathcal{C} \in supp(\mu)$, $\mathcal{C} \Longrightarrow \nu_{\mathcal{C}}$ for some $\nu_{\mathcal{C}}$ such that $\nu = \sum_{\mathcal{C}\in supp(\mu)} \mu(\mathcal{C})\nu_{\mathcal{C}}$.

For any $\mu, \nu \in D(Con)$ and $s = \alpha_1 \ldots \alpha_n \in Act^*$, we say that μ can evolve into ν by a weak s-transition, denoted by $\mu \stackrel{s}{\Longrightarrow} \nu$, if there exist $\mu_1, \ldots, \mu_{n+1}, \nu_1, \ldots, \nu_n \in D(Con)$, such that $\mu \Longrightarrow \mu_1$, $\mu_{n+1} = \nu$, and for each $i = 1, \ldots, n$, $\mu_i \stackrel{\alpha_i}{\longrightarrow} \nu_i$ and $\nu_i \Longrightarrow \mu_{i+1}$.

Lemma 4.2 *Let $\mu = \boxplus_{i\in I} p_i \bullet \mathcal{C}_i$ and $s \in Act^*$. Then $\mu \stackrel{s}{\Longrightarrow} \nu$ if and only for each $i \in I$, $\mathcal{C}_i \stackrel{s}{\Longrightarrow} \nu_i$ for some ν_i such that $\sum_{i\in I} p_i \nu_i = \nu$.*

Proof. Direct to check. □

Note that $\mu \Longrightarrow\stackrel{\alpha}{\longrightarrow} \nu$ and $\mu \stackrel{\alpha}{\Longrightarrow} \nu$ are different since in the former the last action of every execution branch from μ to ν must be α while in the latter the action α appeared in each branch is not necessarily the last one.

With these notations, we can extend Lemma 3.3 to the weak transition case.

Lemma 4.3 *If $\langle P, \rho\rangle \stackrel{s}{\Longrightarrow} \mu$, then*

(1) $\mathrm{tr}(\rho) = \mathrm{tr}(\mu)$*;*

(2) there exist a set of super-operators $\{\mathcal{E}_i : i \in I\}$ acting on $\mathcal{H}_{qv(P)\cup bv(s)}$ where $bv(\alpha_1 \ldots \alpha_n) = bv(\alpha_1) \cup \cdots \cup bv(\alpha_n)$, such that for any $\sigma \in \mathcal{D}(\mathcal{H})$;

$$\langle P, \sigma\rangle \stackrel{s}{\Longrightarrow} \boxplus_{i\in I} q_i^\sigma \bullet \langle P_i, \mathcal{E}_i(\sigma)/q_i^\sigma\rangle$$

where $q_i^\sigma = \mathrm{tr}(\mathcal{E}_i(\sigma))/\mathrm{tr}(\sigma)$;

(3) for any super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{qv(P)\cup bv(s)}}$, we have $\langle P, \mathcal{E}(\rho)\rangle \stackrel{s}{\Longrightarrow} \mathcal{E}(\mu)$.

Proof. We first note from Lemma 3.3(1) that if $\nu \stackrel{\alpha}{\longrightarrow} \mu$, then $\mathrm{tr}(\nu) = \mathrm{tr}(\mu)$. So to prove (1), we need only to show $\mathrm{tr}(\nu) = \mathrm{tr}(\mu)$ provided that $\nu \Longrightarrow \mu$.

Suppose $\langle P, \rho\rangle \Longrightarrow \mu$. If $\mu = \langle P, \rho\rangle$, then $\mathrm{tr}(\rho) = \mathrm{tr}(\mu)$ holds trivially. Otherwise by definition 4.1, we have $\langle P, \rho\rangle \stackrel{\tau}{\longrightarrow} \boxplus_{i\in I} p_i \bullet \mathcal{C}_i$, $\mathcal{C}_i \Longrightarrow \mu_i$ for each $i \in I$, and $\mu = \sum_{i\in I} p_i \mu_i$. Then

$$\begin{aligned}
\mathrm{tr}(\mu) &= \sum_{i\in I} p_i \mathrm{tr}(\mu_i) & \\
&= \sum_{i\in I} p_i \mathrm{tr}(\mathcal{C}_i) & \text{By induction} \\
&= \mathrm{tr}(\rho) & \text{By Lemma 3.3(1).}
\end{aligned}$$

Now if $\nu = \boxplus_{j\in J} q_j \bullet \langle P_j, \rho_j\rangle$ and $\nu \Longrightarrow \mu$, then for each $j \in J$, $\langle P_j, \rho_j\rangle \Longrightarrow \mu_j$ for some μ_j, and $\mu = \sum_{j\in J} q_j \mu_j$. So $\mathrm{tr}(\nu) = \sum_{j\in J} q_j \mathrm{tr}(\rho_j) = \sum_{j\in J} q_j \mathrm{tr}(\mu_j) = \mathrm{tr}(\mu)$.

The proofs of Lemma 4.3(2) and (3) are more complicated, but the idea is similar. So we omit the detail here. □

4.1 Bisimulation

To present the notion of bisimulation, we need a definition from [2].

Definition 4.4 *Let $\mathcal{R} \subseteq Con \times Con$ be a relation on Con, and $\mu, \nu \in D(Con)$. A weight function for (μ, ν) w.r.t. $\mathcal{R}$ is a function $\delta : supp(\mu) \times supp(\nu) \to [0, 1]$ which satisfies*

(1) For all $\mathcal{C}, \mathcal{D} \in Con$,

$$\sum_{\mathcal{D} \in supp(\nu)} \delta(\mathcal{C}, \mathcal{D}) = \mu(\mathcal{C}), \qquad \sum_{\mathcal{C} \in supp(\mu)} \delta(\mathcal{C}, \mathcal{D}) = \nu(\mathcal{D});$$

(2) If $\delta(\mathcal{C}, \mathcal{D}) > 0$, then $(\mathcal{C}, \mathcal{D}) \in \mathcal{R}$.

We write $\mu \mathcal{R} \nu$ if there exists a weight function for (μ, ν) w.r.t. $\mathcal{R}$.

Lemma 4.5 *[2] Suppose $\mu, \nu, \omega \in D(Con)$, $\mathcal{R}, \mathcal{R}' \subseteq Con \times Con$.*

(1) $\mu \mathcal{R} \nu$ if and only if $\nu \mathcal{R}^{-1} \mu$;

(2) $\mu \mathcal{R} \nu$ and $\nu \mathcal{R}' \omega$, then $\mu \mathcal{R} \circ \mathcal{R}' \omega$;

(3) If $\mathcal{R} \subseteq \mathcal{R}'$, then $\mu \mathcal{R} \nu$ implies $\mu \mathcal{R}' \nu$.

Lemma 4.6 *Let $\mu, \nu \in D(Con)$. Then $\mu \mathcal{R} \nu$ if and only if $\mu = \sum_{i \in I} p_i \mathcal{C}_i$ and $\nu = \sum_{i \in I} p_i \mathcal{D}_i$ such that $\mathcal{C}_i \mathcal{R} \mathcal{D}_i$ for each $i \in I$. In particular, if $\mathcal{C} \mathcal{R} \mu$ then $\mathcal{C} \mathcal{R} \mathcal{D}$ for each $\mathcal{D} \in supp(\mu)$.*

Note that when we write $\mu = \sum_{i \in I} p_i \mathcal{C}_i$, then $\mathcal{C}_i$ denotes a simple distribution. As a consequence, the $\mathcal{C}_i$s are not necessarily distinct.

Proof. Let $\mu \mathcal{R} \nu$, and δ is a weight function for (μ, ν) w.r.t. $\mathcal{R}$. Then we have

$$\begin{aligned} \mu &= \sum_{\mathcal{C} \in supp(\mu)} \mu(\mathcal{C}) \mathcal{C} \\ &= \sum_{\mathcal{C} \in supp(\mu)} \sum_{\mathcal{D} \in supp(\nu)} \delta(\mathcal{C}, \mathcal{D}) \mathcal{C} && \text{By Definition 4.4(1)} \\ &= \sum_{\mathcal{C} \mathcal{R} \mathcal{D}} \delta(\mathcal{C}, \mathcal{D}) \mathcal{C} && \text{By Definition 4.4(2).} \end{aligned}$$

Similarly, $\nu = \sum_{\mathcal{C} \mathcal{R} \mathcal{D}} \delta(\mathcal{C}, \mathcal{D}) \mathcal{D}$. That proves the necessity part.

Conversely, suppose $\mu = \sum_{i \in I} p_i \mathcal{C}_i$ and $\nu = \sum_{i \in I} p_i \mathcal{D}_i$ where $\mathcal{C}_i \mathcal{R} \mathcal{D}_i$ for each $i \in I$. We construct a function $\delta : supp(\mu) \times supp(\nu) \to [0, 1]$ such that

$$\delta(\mathcal{C}, \mathcal{D}) = \sum_{i \in I} \{| p_i : \mathcal{C}_i = \mathcal{C} \text{ and } \mathcal{D}_i = \mathcal{D} |\}.$$

Here $\{| \ldots |\}$ denotes a multiset. Then for any $\mathcal{C} \in supp(\mu)$,

$$\sum_{\mathcal{D} \in supp(\nu)} \delta(\mathcal{C}, \mathcal{D}) = \sum_{i \in I} \{| p_i : \mathcal{C}_i = \mathcal{C} |\} = \mu(\mathcal{C}),$$

and similarly, for any $\mathcal{D} \in supp(\nu)$, $\sum_{\mathcal{C} \in supp(\mu)} \delta(\mathcal{C}, \mathcal{D}) = \nu(\mathcal{D})$. Furthermore, if $\delta(\mathcal{C}, \mathcal{D}) > 0$, then $\mathcal{C}_i = \mathcal{C}$ and $\mathcal{D}_i = \mathcal{D}$ for some $i \in I$. Thus $\mathcal{C} \mathcal{R} \mathcal{D}$ by the assumption that $\mathcal{C}_i \mathcal{R} \mathcal{D}_i$. $\square$

Definition 4.7 *A relation $\mathcal{R} \subseteq Con \times Con$ is called a bisimulation if for any $\langle P, \rho\rangle, \langle Q, \sigma\rangle \in Con$, $\langle P, \rho\rangle \mathcal{R} \langle Q, \sigma\rangle$ implies that $qv(P) = qv(Q)$, $\mathrm{tr}_{qv(P)}(\rho) = \mathrm{tr}_{qv(Q)}(\sigma)$, and*

(1) whenever $\langle P, \rho\rangle \xrightarrow{\mathsf{c}?q} \mu$, then $\langle Q, \sigma\rangle \Longrightarrow\xrightarrow{\mathsf{c}?q} \nu$ for some ν such that for any super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{qv(\mu)-\{q\}}}$, $\mathcal{E}(\mu) \mathcal{R} \mathcal{E}(\nu)$;

(2) whenever $\langle P, \rho\rangle \xrightarrow{\alpha} \mu$ where α is not a quantum input, then there exists ν such that $\langle Q, \sigma\rangle \stackrel{\widehat{\alpha}}{\Longrightarrow} \nu$ and $\mu \mathcal{R} \nu$;

(3) whenever $\langle Q, \sigma\rangle \xrightarrow{\mathsf{c}?q} \nu$, then $\langle P, \rho\rangle \Longrightarrow\xrightarrow{\mathsf{c}?q} \mu$ for some μ such that for any super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{qv(\nu)-\{q\}}}$, $\mathcal{E}(\mu) \mathcal{R} \mathcal{E}(\nu)$;

(4) whenever $\langle Q, \sigma\rangle \xrightarrow{\alpha} \nu$ where α is not a quantum input, then there exists μ such that $\langle P, \rho\rangle \stackrel{\widehat{\alpha}}{\Longrightarrow} \mu$ and $\mu \mathcal{R} \nu$.

Definition 4.8 *(1) Two quantum configurations $\langle P, \rho\rangle$ and $\langle Q, \sigma\rangle$ are bisimilar, denoted by $\langle P, \rho\rangle \approx \langle Q, \sigma\rangle$, if there exists a bisimulation $\mathcal{R}$ such that $\langle P, \rho\rangle \mathcal{R} \langle Q, \sigma\rangle$;*

(2) Two quantum processes P and Q are bisimilar, denoted by $P \approx Q$, if for any quantum state $\rho \in \mathcal{D}(\mathcal{H})$ and any indexed set $\widetilde{v}$ of classical values, $\langle P\{\widetilde{v}/\widetilde{x}\}, \rho\rangle \approx \langle Q\{\widetilde{v}/\widetilde{x}\}, \rho\rangle$. Here $\widetilde{x}$ is the set of free classical variables contained in P and Q.

Some design decisions made in Definition 4.7 deserve justification and explanation:

- Recall that in the definition of bisimulations proposed in [5], a clause

$$\text{If } \langle P, \rho\rangle \not\longrightarrow \text{ and } \langle Q, \sigma\rangle \not\longrightarrow, \text{ then } \rho = \sigma \tag{3}$$

is presented to guarantee that the quantum operations applied by P and Q, which give rise only to invisible actions, are the same. That definition, however, does not fit well with recursive definitions since recursively defined processes will generally never reach a terminating process.

In Definition 4.7, we solve this problem by requiring instead that

$$\mathrm{tr}_{qv(P)}(\rho) = \mathrm{tr}_{qv(Q)}(\sigma). \tag{4}$$

Obviously, when $\langle P, \rho\rangle \not\longrightarrow$ and $\langle Q, \sigma\rangle \not\longrightarrow$, and P and Q do not hold any quantum variables, Eqs. (3) and (4) are equivalent. However, Eq.(4) can deal with processes which have infinite behaviors. For example, let

$$A \stackrel{def}{=} \mathsf{c}?q.Set_0[q].\mathsf{c}!q.A$$

and

$$B \stackrel{def}{=} \mathsf{c}?q.M_{0,1}[q;x].\sum_{i=0}^{1}(\mathbf{if}\ x = \lambda_i\ \mathbf{then}\ \sigma_i[q].\mathsf{c}!q.B)$$

where Set_0 is the super-operator which sets the target qubit to $|0\rangle$, and $M_{0,1}$ is the measurement according to the computational basis; that is, $M_{0,1} = \lambda_0|0\rangle\langle 0| + \lambda_1|1\rangle\langle 1|$. Intuitively, B can be regarded as an implementation of A specifying how to set the input qubit to $|0\rangle$. We now show $A \approx B$ indeed holds under our definition of bisimulation. Let

$$\begin{aligned} Con_{0,\rho} &= \{\langle A, \rho\rangle, \langle B, \rho\rangle\} \\ Con_{1,q,\rho} &= \{\langle A_{1q}, \rho\rangle, \langle A_{2q}, \rho_0\rangle, \langle B_{1q}, \rho\rangle, \langle B_{2qj}, \rho_j\rangle, \langle B_{3q}, \rho_0\rangle : j = 0, 1\} \end{aligned}$$

where $A_{1q} = Set_0[q].\mathsf{c}!q.A$, $A_{2q} = \mathsf{c}!q.A$,

$$\begin{aligned} B_{1q} &= M_{0,1}[q;x].\sum_{i=0}^{1}(\textbf{if } x = \lambda_i \textbf{ then } \sigma_i[q].\mathsf{c}!q.B), \\ B_{2qj} &= \sum_{i=0}^{1}(\textbf{if } \lambda_j = \lambda_i \textbf{ then } \sigma_i[q].\mathsf{c}!q.B), \end{aligned}$$

$B_{3q} = \mathsf{c}!q.B$, and $\rho_j = [|j\rangle]_q \otimes \mathrm{tr}_q\rho$. Let $\mathcal{R} \subseteq Con \times Con$ such that $\langle P, \sigma\rangle \mathcal{R} \langle Q, \eta\rangle$ if and only if there exist $q \in qVar$ and $\rho \in \mathcal{D}(\mathcal{H})$ such that $\langle P, \sigma\rangle$ and $\langle Q, \eta\rangle$ are simultaneously included in $Con_{0,\rho}$ or $Con_{1,q,\rho}$. Then it is not difficult to prove that $\mathcal{R}$ is a bisimulation. Thus $A \approx B$.

- Furthermore, by replacing Eq.(3) with Eq.(4), the derived bisimilarity will be preserved by restriction. Take the example in [5]. Let U_1, U_2, V_1, V_2 be unitary operators such that $U_2U_1 = V_2V_1$ but $U_1 \neq V_1$. Let

$$P = U_1[q].c!0.U_2[q].\textbf{nil}, Q = V_1[q].c!0.V_2[q].\textbf{nil}.$$

  Then P and Q are bisimilar but $P\backslash\{c\}$ and $Q\backslash\{c\}$ are not if Eq.(3) is required in the definition. However, in our definition presented here, $P\backslash\{c\}$ and $Q\backslash\{c\}$ are also bisimilar since in Eq.(4) we only need to consider the reduced states on the systems $\overline{qv(P)} = \overline{qv(Q)}$. The "unfinished" quantum operations, which are blocked by the restriction, are not taken into account when comparing the accompanying quantum states.

- Another question one may ask is that why we require $qv(P) = qv(Q)$ in the definition, which excludes the pair

$$P = I[q].\textbf{nil} \quad \text{and} \quad Q = \textbf{nil}$$

  to be bisimilar. The reason is, although P and Q have the same effect (they both do nothing at all) on the environment, they are indeed different under parallel composition. For example, if $q \in qv(R)$, then the process $Q\|R$ is valid while $P\|R$ is not.

- In Clause (1), we require $\mathcal{E}(\mu)\mathcal{R}\mathcal{E}(\nu)$ for any super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{qv(\mu)-\{q\}}}$. The reason for this rather strange requirement is as follows. To check whether two configurations are bisimilar, we have to feed them with all possible inputs. In classical process algebra, this is realized by requiring that the input value is arbitrarily chosen. In quantum process algebra, however, since the state of all environmental systems is fixed for a given configuration, only requiring the arbitrariness of the input system is not sufficient. Note that the state-preparation operation and the swap operation are both special super-operators. Our definition actually includes the possibility of inputing an arbitrary system which lies in an arbitrary state.

  Furthermore, this requirement is also essential in proving the congruence property of the derived bisimilarity (See Theorem 4.18).

Example 4.9 (Superdense coding revisited) This example is devoted to proving rigorously that the protocol presented in Example 3.4 indeed sends two bits of classical information from Alice to Bob by transmitting a qubit, with the help of a maximally entangled state. Let

$$Sdc_{spec} = c?x.Set_x[q_1, q_2].d!x.\textbf{nil}$$

be the specification of superdense coding protocol, where

$$Set_x[q_1, q_2].d!x.\textbf{nil} = \sum_{i=0}^{3}(\textbf{if } x = i \textbf{ then } Set_i[q_1, q_2].d!x.\textbf{nil}),$$

and Set_i, $i = 0, \ldots, 3$, is the 2-qubit super-operator which sets the target qubits to $|\widetilde{i}\rangle$; that is, for any $\rho \in \mathcal{D}(\mathcal{H})$,

$$Set_{i,q,q'}(\rho) = [|\widetilde{i}\rangle]_{q,q'} \otimes \mathrm{tr}_{q,q'}(\rho).$$

We have $Set_x[q_1, q_2]$ in the specification simply for technical reasons: to make $qv(Sdc_{spec}) = qv(Sdc)$ and to set q_1, q_2 to the required final states. For any $\rho \in \mathcal{D}(\mathcal{H}_{\overline{\{q_1,q_2\}}})$, and $v \in \{0, 1, 2, 3\}$,

$$\begin{aligned}
& \langle Sdc_{spec}, [|\Psi\rangle]_{q_1,q_2} \otimes \rho\rangle \\
\xrightarrow{c?v} \ & \langle Set_v[q_1, q_2].d!v.\mathbf{nil}, [|\Psi\rangle]_{q_1,q_2} \otimes \rho\rangle \\
\xrightarrow{\tau} \ & \langle d!v.\mathbf{nil}, [|\widetilde{v}\rangle]_{q_1,q_2} \otimes \rho\rangle \\
\xrightarrow{d!v} \ & \langle \mathbf{nil}, [|\widetilde{v}\rangle]_{q_1,q_2} \otimes \rho\rangle.
\end{aligned}$$

We can easily prove

$$\langle Sdc, [|\Psi\rangle]_{q_1,q_2} \otimes \rho\rangle \approx \langle Sdc_{spec}, [|\Psi\rangle]_{q_1,q_2} \otimes \rho\rangle$$

by checking that

$$\begin{aligned}
\mathcal{R} \ = \ & \{(\langle Sdc, \rho_\Psi\rangle, \langle Sdc_{spec}, \rho_\Psi\rangle)\} \\
& \cup\{(\langle P, \eta\rangle, \langle Set_v[q_1, q_2].d!v.\mathbf{nil}, \rho_\Psi\rangle) : v = 0, \ldots, 3, \\
& \quad \langle Sdc, \rho_\Psi\rangle \overset{c?v}{\Longrightarrow} \langle P, \eta\rangle, \text{ and } qv(P) \neq \emptyset\} \\
& \cup\{(\langle(\mathbf{nil}\|d!v.\mathbf{nil})\backslash\{\mathsf{e}\}, \rho_{\widetilde{v}}\rangle, \langle d!v.\mathbf{nil}, \rho_{\widetilde{v}}\rangle) : v = 0, \ldots, 3\} \\
& \cup\{(\langle(\mathbf{nil}\|\mathbf{nil})\backslash\{\mathsf{e}\}, \rho_{\widetilde{v}}\rangle, \langle \mathbf{nil}, \rho_{\widetilde{v}}\rangle) : v = 0, \ldots, 3\}
\end{aligned}$$

is a bisimulation, where $\rho_\psi = [|\psi\rangle]_{q_1,q_2} \otimes \rho$.

Note that $Sdc \approx Sdc_{spec}$ does not hold in general since superdense coding protocol needs the assistance of a maximally entangled state to realize the intended task.

Example 4.10 (Teleportation revisited) This example is devoted to proving rigorously that the protocol presented in Example 3.5 indeed teleports any unknown quantum state from Alice to Bob, again with the help of a maximally entangled state. To employ our notion of bisimulation, we need to modify the original definition of Alice's protocol in Example 3.5 as follows:

$$Alice'_t = \mathsf{c}?q.CN[q, q_1].H[q].M[q, q_1; x].Set_\Psi[q, q_1].e!x.\mathbf{nil}$$

and $Tel' = (Alice'_t\|Bob_t)\backslash c$ where Set_Ψ is similar to Set_x in the previous example. Let

$$Tel_{spec} = \mathsf{c}?q.SWAP_{1,3}[q, q_1, q_2].\mathsf{d}!q_2.\mathbf{nil}$$

be the specification of teleportation protocol, where $SWAP_{1,3}$ is a 3-qubit unitary operator which exchanges the states of the first and the third qubits, keeping the second qubit untouched. Again, we involve qubit q_1 here just for technique reason: to make $qv(Tel_{spec}) = qv(Tel')$. Then for any $\rho \in \mathcal{D}(\mathcal{H}_{\overline{\{q_1,q_2\}}})$ and $r \neq q_1, q_2$,

$$\begin{aligned}
& \langle Tel_{spec}, [|\Psi\rangle]_{q_1,q_2} \otimes \rho\rangle \\
\xrightarrow{\mathsf{c}?r} \ & \langle SWAP_{1,3}[r, q_1, q_2].\mathsf{d}!q_2.\mathbf{nil}, [|\Psi\rangle]_{q_1,q_2} \otimes \rho\rangle \\
\xrightarrow{\tau} \ & \langle \mathsf{d}!q_2.\mathbf{nil}, [|\Psi\rangle]_{q_1,r} \otimes \rho\rangle \\
\xrightarrow{\mathsf{d}!q_2} \ & \langle \mathbf{nil}, [|\Psi\rangle]_{q_1,r} \otimes \rho\rangle.
\end{aligned}$$

We can now prove

$$\langle Tel', [|\Psi\rangle]_{q_1,q_2} \otimes \rho\rangle \approx \langle Tel_{spec}, [|\Psi\rangle]_{q_1,q_2} \otimes \rho\rangle$$

by checking that

$$\begin{aligned}
\mathcal{R} \ = \ & \{(\langle Tel', \rho_\Psi^{q_1,q_2}\rangle, \langle Tel_{spec}, \rho_\Psi^{q_1,q_2}\rangle)\} \\
& \cup\{(\langle P,\eta\rangle, \langle SWAP_{1,3}[r,q_1,q_2].\mathsf{d}!q_2.\mathbf{nil}, \sigma_\Psi^{q_1,q_2}) : \\
& \quad \langle Tel', \sigma_\Psi^{q_1,q_2}\rangle \stackrel{\mathsf{c}?r}{\Longrightarrow} \langle P,\eta\rangle, \sigma \in \mathcal{D}(\mathcal{H}_{\overline{\{q_1,q_2\}}}), \\
& \quad qv(P) = \{r, q_1, q_2\}, \text{ and } r \neq q_1, q_2\} \\
& \cup\{(\langle P,\eta\rangle, \langle \mathsf{d}!q_2.\mathbf{nil}, \sigma_\Psi^{q_1,r}) : \\
& \quad \langle Tel', \sigma_\Psi^{q_1,q_2}\rangle \stackrel{\mathsf{c}?r}{\Longrightarrow} \mu \text{ with } \langle P,\eta\rangle \in supp(\mu), \\
& \quad \sigma \in \mathcal{D}(\mathcal{H}_{\overline{\{q_1,q_2\}}}), qv(P) = \{q_2\}, \text{ and } r \neq q_1, q_2\} \\
& \cup\{(\langle(\mathbf{nil}\|\mathbf{nil})\backslash\{c\}, \sigma_\Psi^{q_1,r}\rangle, \langle \mathbf{nil}, \sigma_\Psi^{q_1,r}\rangle) : \sigma \in \mathcal{D}(\mathcal{H}_{\overline{\{q_1,r\}}})\}
\end{aligned}$$

is a bisimulation, where $\sigma_\psi^{q,q'} = [|\psi\rangle]_{q,q'} \otimes \sigma$.

Again, $Tel' \approx Tel_{spec}$ does not hold in general since Teleportation protocol is valid only when a maximally entangled state is provided and consumed.

The following example shows the bimilarity between quantum processes.

Example 4.11 (Encode quantum circuits by qCCS, revisited) Using the notion presented in Example 3.6, we can prove the following properties considering the sequential composition and parallel composition of quantum gates:

(1) $\mathcal{U}(U) \circ \mathcal{U}(V) \approx \mathcal{U}(VU)$;

(2) $\mathcal{U}(U) \circ \mathcal{G}(M) \approx \mathcal{G}(U^\dagger M U) \circ \mathcal{U}(U)$;

(3) $\mathcal{U}(U) \otimes \mathcal{U}(V) \approx \mathcal{U}(V \otimes V)$.

The proof is straightforward, and we only take (1) as an example. Let

$$\begin{aligned}
\mathcal{R} \ = \ & \{(\langle \mathcal{U}(U) \circ \mathcal{U}(V), \rho\rangle, \langle \mathcal{U}(VU), \rho\rangle) : \rho \in \mathcal{D}(\mathcal{H})\} \\
\cup \ & \{(\langle P,\sigma\rangle, \langle Q,\eta\rangle) : \langle \mathcal{U}(U) \circ \mathcal{U}(V), \rho\rangle \stackrel{\mathsf{c}^n?\widetilde{r}}{\Longrightarrow} \langle P,\sigma\rangle \text{ and} \\
& \langle \mathcal{U}(VU), \rho\rangle \stackrel{\mathsf{c}^n?\widetilde{r}}{\Longrightarrow} \langle Q,\eta\rangle \text{ where } \widetilde{r} \subseteq qVar \text{ and } \rho \in \mathcal{D}(\mathcal{H})\} \\
\cup \ & \{(\langle P,\sigma\rangle, \langle Q,\eta\rangle) : \langle \mathcal{U}(U) \circ \mathcal{U}(V), \rho\rangle \stackrel{\mathsf{c}^n?\widetilde{r},\mathsf{d}^n!\widetilde{r}}{\Longrightarrow} \langle P,\sigma\rangle \text{ and} \\
& \langle \mathcal{U}(VU), \rho\rangle \stackrel{\mathsf{c}^n?\widetilde{r},\mathsf{d}^n!\widetilde{r}}{\Longrightarrow} \langle Q,\eta\rangle \text{ where } \widetilde{r} \subseteq qVar \text{ and } \rho \in \mathcal{D}(\mathcal{H})\}.
\end{aligned}$$

It is easy to check that $\mathcal{R}$ is a bisimulation. So we have $\langle \mathcal{U}(U) \circ \mathcal{U}(V), \rho\rangle \approx \langle \mathcal{U}(VU), \rho\rangle$ for all $\rho \in \mathcal{D}(\mathcal{H})$ and then $\mathcal{U}(U) \circ \mathcal{U}(V) \approx \mathcal{U}(VU)$.

To conclude this section, we prove some properties of bisimilarity which are useful in the rest of this paper.

Lemma 4.12 *Let $\mathcal{R}$ be a bisimulation, and $\mu\mathcal{R}\nu$.*

(1) If $\mu \Longrightarrow\stackrel{\mathsf{c}?q}{\longrightarrow} \mu'$, then $\nu \Longrightarrow\stackrel{\mathsf{c}?q}{\longrightarrow} \nu'$ for some ν' such that for any super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{qv(\mu')-\{q\}}}$, $\mathcal{E}(\mu')\mathcal{R}\mathcal{E}(\nu')$;

(2) If $\mu \stackrel{\alpha}{\Longrightarrow} \mu'$ where α is not a quantum input, then there exists ν' such that $\nu \stackrel{\widehat{\alpha}}{\Longrightarrow} \nu'$ and $\mu'\mathcal{R}\nu'$.

Proof. Easy from Lemma 4.6, noting that $\mu \stackrel{s}{\Longrightarrow} \nu$ if and only for any $\mathcal{C} \in supp(\mu)$, $\mathcal{C} \stackrel{s}{\Longrightarrow} \nu_{\mathcal{C}}$ with $\nu = \sum_{\mathcal{C}\in supp(\mu)} \mu(\mathcal{C})\nu_{\mathcal{C}}$. □

Theorem 4.13 *$\approx$ is a bisimulation on Con, and it is an equivalence relation.*

Proof. Let each $\mathcal{R}_i, (i = 1, 2, \dots)$ be a bisimulation on Con. From Lemmas 4.5 and 4.12, we can prove that the following relations are all bisimulations:

$$\begin{array}{ll} (1)\ Id_{Con} & (2)\ \mathcal{R}_i^{-1} \\ (3)\ \mathcal{R}_1 \circ \mathcal{R}_2 & (4)\ \bigcup_i \mathcal{R}_i. \end{array}$$

Then the result follows. □

Theorem 4.14 *For any configurations $\langle P, \rho\rangle$ and $\langle Q, \sigma\rangle$, $\langle P, \rho\rangle \approx \langle Q, \sigma\rangle$ if and only if $qv(P) = qv(Q)$, $\mathrm{tr}_{qv(P)}(\rho) = \mathrm{tr}_{qv(Q)}(\sigma)$, and*

(1) whenever $\langle P, \rho\rangle \xrightarrow{c?q} \mu$, then $\langle Q, \sigma\rangle \Longrightarrow\xrightarrow{c?q} \nu$ for some ν such that for any super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{qv(\mu)-\{q\}}}$, $\mathcal{E}(\mu) \approx \mathcal{E}(\nu)$;

(2) whenever $\langle P, \rho\rangle \xrightarrow{\alpha} \mu$ where α is not a quantum input, then there exists ν such that $\langle Q, \sigma\rangle \stackrel{\widehat{\alpha}}{\Longrightarrow} \nu$ and $\mu \approx \nu$;

and the symmetric conditions of (1) and (2).

Proof. Similar to the corresponding result, Theorem 36, of [5]. □

Lemma 4.15 *If $\langle P, \rho\rangle \approx \langle Q, \sigma\rangle$, then for any super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{qv(P)}}$, we have $\mathrm{tr}(\mathcal{E}(\rho)) = \mathrm{tr}(\mathcal{E}(\sigma))$. In particular, $\mathrm{tr}(\rho) = \mathrm{tr}(\sigma)$.*

Proof. Let $S = qv(P)$. From $\langle P, \rho\rangle \approx \langle Q, \sigma\rangle$, we have $\mathrm{tr}_S(\rho) = \mathrm{tr}_S(\sigma)$. Note that $\mathcal{E}(\mathrm{tr}_S(\rho)) = \mathrm{tr}_S(\mathcal{E}(\rho))$ since $\mathcal{E}$ acts only on $\mathcal{H}_{\overline{S}}$, and $\mathrm{tr}(\mathcal{E}(\rho)) = \mathrm{tr}_{\overline{S}}(\mathrm{tr}_S(\mathcal{E}(\rho)))$. The result follows. □

As in classical process algebra, the notion of bisimulation up to $\approx$ can be defined:

Definition 4.16 *A relation $\mathcal{R} \subseteq Con \times Con$ is called a bisimulation up to $\approx$ if for any $\langle P, \rho\rangle, \langle Q, \sigma\rangle \in Con$, $\langle P, \rho\rangle\mathcal{R}\langle Q, \sigma\rangle$ implies that $qv(P) = qv(Q)$, $\mathrm{tr}_{qv(P)}(\rho) = \mathrm{tr}_{qv(Q)}(\sigma)$, and*

(1) whenever $\langle P, \rho\rangle \xrightarrow{c?q} \mu$, then $\langle Q, \sigma\rangle \Longrightarrow\xrightarrow{c?q} \nu$ for some ν such that for any super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{qv(\mu)-\{q\}}}$, $\mathcal{E}(\mu)\mathcal{R}\circ \approx\mathcal{E}(\nu)$;

(2) whenever $\langle P, \rho\rangle \xrightarrow{\alpha} \mu$ where α is not a quantum input, then there exists ν such that $\langle Q, \sigma\rangle \stackrel{\widehat{\alpha}}{\Longrightarrow} \nu$ and $\mu\mathcal{R}\circ \approx\nu$;

and the symmetric conditions of (1) and (2).

Lemma 4.17 *If $\mathcal{R}$ is a bisimulation up to $\approx$, then $\mathcal{R} \subseteq\approx$.*

Proof. Suppose $\mathcal{R}$ is a bisimulation up to $\approx$. We first prove that that $\mathcal{R}\circ \approx$ is a bisimulation. Let $\langle P, \rho\rangle\mathcal{R}\circ \approx \langle Q, \sigma\rangle$; that is, there exists $\langle R, \eta\rangle$ such that $\langle P, \rho\rangle\mathcal{R}\langle R, \eta\rangle$ and $\langle R, \eta\rangle \approx \langle Q, \sigma\rangle$. Then $qv(P) = qv(R) = qv(Q)$, and $\mathrm{tr}_{qv(P)}(\rho) = \mathrm{tr}_{qv(R)}(\eta) = \mathrm{tr}_{qv(Q)}(\sigma)$.

Let $\langle P, \rho\rangle \xrightarrow{c?q} \mu$. Then $\langle R, \eta\rangle \Longrightarrow\xrightarrow{c?q} \omega$ such that for any super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{qv(\mu)-\{q\}}}$, $\mathcal{E}(\mu)\mathcal{R}\circ \approx\mathcal{E}(\omega)$. We further derive from Lemma 4.12 that $\langle Q, \sigma\rangle \Longrightarrow\xrightarrow{c?q} \nu$, and for any super-operator $\mathcal{F}$ acting on $\mathcal{H}_{\overline{qv(\omega)-\{q\}}}$, $\mathcal{F}(\omega)\approx\mathcal{F}(\nu)$. Note that $qv(\mu) = qv(\omega)$. We have $\mathcal{E}'(\mu)\mathcal{R}\circ \approx\mathcal{E}'(\nu)$ for any super-operator $\mathcal{E}'$ acting on $\mathcal{H}_{\overline{qv(\mu)-\{q\}}}$, by Lemma 4.5.

Let $\langle P, \rho\rangle \xrightarrow{\alpha} \mu$ for some α not a quantum input. Then $\langle R, \eta\rangle \stackrel{\widehat{\alpha}}{\Longrightarrow} \nu$ such that $\mu\mathcal{R}\circ \approx\nu$. Furthermore, from $\langle R, \eta\rangle \approx \langle Q, \sigma\rangle$ we have $\langle Q, \sigma\rangle \stackrel{\widehat{\alpha}}{\Longrightarrow} \omega$ such that $\nu\approx\omega$, by Lemma 4.12. So we have $\mu\mathcal{R}\circ \approx\omega$ from Lemma 4.5.

The symmetric form when $\langle Q, \sigma\rangle \xrightarrow{\alpha}$ can be similarly proved. So $\mathcal{R}\circ \approx$ is a bisimulation; that is, $\mathcal{R}\circ \approx\subseteq\approx$. Then the result holds by noting that the identity relation is a trivial bisimulation. $\square$

4.2 Bisimilarity congruence

We now turn to prove the congruence properties of bisimulation. First, we show that the bisimulation for configurations is preserved by all *static* constructors.

Theorem 4.18 *If $\langle P, \rho\rangle \approx \langle Q, \sigma\rangle$ then*

(1) $\langle P\|R, \rho\rangle \approx \langle Q\|R, \sigma\rangle$;

(2) $\langle P[f], \rho\rangle \approx \langle Q[f], \sigma\rangle$;

(3) $\langle P\backslash L, \rho\rangle \approx \langle Q\backslash L, \sigma\rangle$;

(4) $\langle \textbf{if } b \textbf{ then } P, \rho\rangle \approx \langle \textbf{if } b \textbf{ then } Q, \sigma\rangle$.

Proof. Let us prove (1); other cases are simpler. Let

$$\mathcal{R} = \{(\langle P\|R, \mathcal{E}(\rho)\rangle, \langle Q\|R, \mathcal{E}(\sigma)\rangle) : \langle P, \rho\rangle \approx \langle Q, \sigma\rangle \text{ and } \mathcal{E} \text{ is a super-operator acting on } \mathcal{H}_{\overline{qv(P)}}\}.$$

It suffices to show that $\mathcal{R}$ is a bisimulation. Suppose $(\mathcal{C}, \mathcal{D}) \in \mathcal{R}$ where $\mathcal{C} = \langle P\|R, \mathcal{E}(\rho)\rangle$ and $\mathcal{D} = \langle Q\|R, \mathcal{E}(\sigma)\rangle$ for some $\langle P, \rho\rangle \approx \langle Q, \sigma\rangle$, and $\mathcal{E}$ is a super-operator acting on $\mathcal{H}_{\overline{qv(P)}}$. Then $qv(P) = qv(Q)$ and $\mathrm{tr}_{qv(P)}(\rho) = \mathrm{tr}_{qv(Q)}(\sigma)$ by Theorem 4.14. Thus $qv(P\|R) = qv(Q\|R)$ and

$$\mathrm{tr}_{qv(P\|R)}(\mathcal{E}(\rho)) = \mathrm{tr}_{qv(Q\|R)}(\mathcal{E}(\sigma)).$$

Let $\langle P\|R, \mathcal{E}(\rho)\rangle \xrightarrow{\alpha} \mu$ for some α and μ. There are three cases to consider.

I: The transition is caused by P solely. We need to further consider two subcases:

i: $\alpha = \mathsf{c}?q$ is a quantum input. Then there exists a transition $\langle P, \rho\rangle \xrightarrow{\mathsf{c}?q} \langle P', \rho\rangle$ and $\mu = \langle P'\|R, \mathcal{E}(\rho)\rangle$. By the assumption that $\langle P, \rho\rangle \approx \langle Q, \sigma\rangle$, we have

$$\langle Q, \sigma\rangle \Longrightarrow \boxplus_{i\in I} p_i \bullet \langle Q_i', \sigma_i\rangle \xrightarrow{\mathsf{c}?q} \boxplus_{i\in I} p_i \bullet \langle Q_i, \sigma_i\rangle$$

such that for any super-operator $\mathcal{F}$ acting on $\mathcal{H}_{\overline{qv(P')-\{q\}}}$,

$$\langle P', \mathcal{F}(\rho)\rangle \approx \langle Q_i, \mathcal{F}(\sigma_i)\rangle \tag{5}$$

holds for any $i \in I$. Then $\langle Q, \mathcal{E}(\sigma)\rangle \Longrightarrow \boxplus_{i\in I} p_i \bullet \langle Q_i', \mathcal{E}(\sigma_i)\rangle$ by Lemma 4.3(3), from which we further derive

$$\langle Q, \mathcal{E}(\sigma)\rangle \Longrightarrow\xrightarrow{\mathsf{c}?q} \boxplus_{i\in I} p_i \bullet \langle Q_i, \mathcal{E}(\sigma_i)\rangle$$

and

$$\langle Q\|R, \mathcal{E}(\sigma)\rangle \Longrightarrow\xrightarrow{\mathsf{c}?q} \nu = \boxplus_{i\in I} p_i \bullet \langle Q_i\|R, \mathcal{E}(\sigma_i)\rangle.$$

For any super-operator $\mathcal{F}'$ acting on $\mathcal{H}_{\overline{qv(P'\|R)-\{q\}}}$, we obtain from Lemma 3.2 that the composite map $\mathcal{F}' \circ \mathcal{E}$ is a super-operator acting on $\mathcal{H}_{\overline{qv(P')-\{q\}}}$. Now using Eq.(5) we have

$$\langle P', \mathcal{F}'(\mathcal{E}(\rho))\rangle \approx \langle Q_i, \mathcal{F}'(\mathcal{E}(\sigma_i))\rangle,$$

and thus $\langle P'\|R, \mathcal{F}'(\mathcal{E}(\rho))\rangle\mathcal{R}\langle Q_i\|R, \mathcal{F}'(\mathcal{E}(\sigma_i))\rangle$. That is, $\mathcal{F}'(\mu)\mathcal{R}\mathcal{F}'(\nu)$ as required.

ii: α is not a quantum input. Then there exists a transition $\langle P, \rho\rangle \xrightarrow{\alpha} \mu_1 = \boxplus_{i\in I} p_i \bullet \langle P_i, \rho_i\rangle$ and $\mu = \boxplus_{i\in I} p_i \bullet \langle P_i \| R, \mathcal{E}(\rho_i)\rangle$ by Lemma 3.3(3). From the assumption that $\langle P, \rho\rangle \approx \langle Q, \sigma\rangle$, we have

$$\langle Q, \sigma\rangle \stackrel{\widehat{\alpha}}{\Longrightarrow} \nu_1 = \boxplus_{j\in J} q_j \bullet \langle Q_j, \sigma_j\rangle$$

and $\mu_1 \approx \nu_1$ by Theorem 4.14. Noting that $\mathcal{E}$ is a super-operator on $\mathcal{H}_{\overline{qv(Q)}}$, we have $\langle Q, \mathcal{E}(\sigma)\rangle \stackrel{\widehat{\alpha}}{\Longrightarrow} \boxplus_{j\in J} q_j \bullet \langle Q_j, \mathcal{E}(\sigma_j)\rangle$ by Lemma 4.3(3). So it holds that

$$\langle Q \| R, \mathcal{E}(\sigma)\rangle \stackrel{\widehat{\alpha}}{\Longrightarrow} \nu = \boxplus_{j\in J} q_j \bullet \langle Q_j \| R, \mathcal{E}(\sigma_j)\rangle.$$

Now for each $i \in I$ and $j \in J$, $\langle P_i, \rho_i\rangle \approx \langle Q_j, \sigma_j\rangle$ implies $\langle P_i \| R, \mathcal{E}(\rho_i)\rangle \mathcal{R} \langle Q_j \| R, \mathcal{E}(\sigma_j)\rangle$ since from Lemma 3.2, $\mathcal{E}$ is also a super-operator acting on $\mathcal{H}_{\overline{qv(P_i)}}$. Thus we have $\mu \mathcal{R} \nu$ by Lemma 4.6, by noting that $\mu_1 \approx \nu_1$.

II: The transition is caused by R solely. We also need to further consider two subcases:

i: $\alpha = \mathsf{c}?q$ is a quantum input where $q \notin qv(P)$. Then we have $\langle R, \mathcal{E}(\rho)\rangle \xrightarrow{\mathsf{c}?q} \langle R', \mathcal{E}(\rho)\rangle$ for some R', and $\mu = \langle P \| R', \mathcal{E}(\rho)\rangle$. Thus $\langle R, \mathcal{E}(\sigma)\rangle \xrightarrow{\mathsf{c}?q} \langle R', \mathcal{E}(\sigma)\rangle$. By inference rule **Inp-Int**, we have

$$\langle Q \| R, \mathcal{E}(\sigma)\rangle \xrightarrow{\mathsf{c}?q} \langle Q \| R', \mathcal{E}(\sigma)\rangle$$

since $q \notin qv(Q)$. Now for any super-operator $\mathcal{F}$ acting on $\mathcal{H}_{\overline{qv(P\|R')-\{q\}}}$, the composite map $\mathcal{F} \circ \mathcal{E}$ is a super-operator acting on $\mathcal{H}_{\overline{qv(P)}}$ from the fact that $qv(P\|R') - \{q\} \supseteq qv(P) - \{q\} = qv(P)$. Thus

$$\langle P \| R', \mathcal{F}(\mathcal{E}(\rho))\rangle \mathcal{R} \langle Q \| R', \mathcal{F}(\mathcal{E}(\sigma))\rangle$$

from the definition of $\mathcal{R}$.

ii: α is not a quantum input. Then by Lemma 3.3(2), there exists a transition $\langle R, \mathcal{E}(\rho)\rangle \xrightarrow{\alpha} \boxplus p_i \bullet \langle R_i, \mathcal{E}_i(\mathcal{E}(\rho))/p_i\rangle$ where $\mathcal{E}_i$ is a super-operator on $\mathcal{H}_{qv(R)}$,

$$p_i = \mathrm{tr}(\mathcal{E}_i(\mathcal{E}(\rho)))/\mathrm{tr}(\mathcal{E}(\rho)),$$

and $\mu = \boxplus p_i \bullet \langle P \| R_i, \mathcal{E}_i(\mathcal{E}(\rho))/p_i\rangle$. Then we derive

$$\langle R, \mathcal{E}(\sigma)\rangle \xrightarrow{\alpha} \boxplus q_i \bullet \langle R_i, \mathcal{E}_i(\mathcal{E}(\sigma))/q_i\rangle$$

where $q_i = \mathrm{tr}(\mathcal{E}_i(\mathcal{E}(\sigma)))/\mathrm{tr}(\mathcal{E}(\sigma))$, again by Lemma 3.3(2). Thus

$$\langle Q \| R, \mathcal{E}(\sigma)\rangle \xrightarrow{\alpha} \nu = \boxplus q_i \bullet \langle Q \| R_i, \mathcal{E}_i(\mathcal{E}(\sigma))/q_i\rangle.$$

Notice that for any i, we have $p_i = q_i$ by Lemma 4.15, and

$$(\langle P \| R_i, \mathcal{E}_i(\mathcal{E}(\rho))\rangle, \langle Q \| R_i, \mathcal{E}_i(\mathcal{E}(\sigma))\rangle) \in \mathcal{R}$$

since the composite map $\mathcal{E}^i \circ \mathcal{E}$ is a super-operator acting on $\mathcal{H}_{\overline{qv(P)}}$ ($qv(R) \cap qv(P) = \emptyset$ by the validity of $P\|R$). Then it follows that $\mu \mathcal{R} \nu$ from Lemma 4.6.

III: The transition is caused by a communication between P and R. Without loss of generality, we assume that

$$\langle P, \rho\rangle \xrightarrow{\mathsf{c}?q} \langle P', \rho\rangle, \quad \langle R, \rho\rangle \xrightarrow{\mathsf{c}!q} \langle R', \rho\rangle,$$

and $\mu = \langle P' \| R', \mathcal{E}(\rho)\rangle$. Other cases are simpler. Then $q \notin qv(P)$ by the validity of $P\|R$, and $\langle R, \eta\rangle \xrightarrow{\mathsf{c}!q} \langle R', \eta\rangle$ for any $\eta \in \mathcal{D}(\mathcal{H})$. From the assumption that $\langle P, \rho\rangle \approx \langle Q, \sigma\rangle$, we have

$$\langle Q, \sigma\rangle \Longrightarrow \boxplus_{i\in I} p_i \bullet \langle Q_i', \sigma_i\rangle \xrightarrow{\mathsf{c}?q} \boxplus_{i\in I} p_i \bullet \langle Q_i, \sigma_i\rangle$$

such that for any $i \in I$ and any super-operator $\mathcal{F}$ acting on $\mathcal{H}_{\overline{qv(P')-\{q\}}}$, it holds that $\langle P', \mathcal{F}(\rho)\rangle \approx \langle Q_i, \mathcal{F}(\sigma_i)\rangle$. In particular, we have

$$\langle P', \mathcal{E}(\rho)\rangle \approx \langle Q_i, \mathcal{E}(\sigma_i)\rangle \tag{6}$$

since $qv(P) \supseteq qv(P') - \{q\}$. Noting that $\mathcal{E}$ is a super-operator on $\mathcal{H}_{\overline{qv(Q)}}$, we have $\langle Q, \mathcal{E}(\sigma)\rangle \Longrightarrow \boxplus_{i\in I} p_i \bullet \langle Q_i', \mathcal{E}(\sigma_i)\rangle$ by Lemma 4.3(3), from which we derive further

$$\langle Q, \mathcal{E}(\sigma)\rangle \Longrightarrow\xrightarrow{\mathsf{c}?q} \boxplus_{i\in I} p_i \bullet \langle Q_i, \mathcal{E}(\sigma_i)\rangle,$$

and

$$\langle Q\|R, \mathcal{E}(\sigma)\rangle \Longrightarrow\xrightarrow{\tau} \nu = \boxplus_{i\in I} p_i \bullet \langle Q_i \| R', \mathcal{E}(\sigma_i)\rangle.$$

Furthermore, for any $i \in I$, we have

$$(\langle P' \| R', \mathcal{E}(\rho)\rangle, \langle Q_i \| R', \mathcal{E}(\sigma_i)\rangle) \in \mathcal{R}$$

by Eq.(6). That is, $\mu \mathcal{R} \nu$ as required.

The symmetric form when $\langle Q\|R, \mathcal{E}(\sigma)\rangle \xrightarrow{\alpha} \nu$ can be similarly proved. So $\mathcal{R}$ is a bisimulation on *Con*. The result follows by noting that the identity transformation is also a super-operator on $\mathcal{H}_{\overline{qv(P)}}$. □

From Theorem 4.18, the superdense coding protocol and teleportation protocol presented in Section 3 is still valid in any quantum process context which consists only of parallel composition, relabeling, restriction, and conditional.

The configuration bisimulation is not preserved, however, by *dynamic* constructors such as prefix and summation. A counterexample is as follows. Let $P = M_{0,1}[q; x].\mathbf{nil}$ where $M_{0,1} = \lambda_0[|0\rangle] + \lambda_1[|1\rangle]$ is the 1-qubit measurement according to the computational basis, $Q = I[q].\mathbf{nil}$, and $\rho = [|0\rangle]_q \otimes \sigma$ where $\sigma \in \mathcal{D}(\mathcal{H}_{\overline{q}})$. Then $\langle P, \rho\rangle \approx \langle Q, \rho\rangle$, but $\langle H[q].P, \rho\rangle \not\approx \langle H[q].Q, \rho\rangle$ where H is the Hadamard operator.

Nevertheless, similar to standard classical CCS, the bisimulation for quantum processes is preserved by all the combinators of qCCS except for summation.

Theorem 4.19 *If $P \approx Q$ then*

(1) $a.P \approx a.Q$, $a \in \{\tau, c?x, c!e, \mathsf{c}?q, \mathsf{c}!q, \mathcal{E}[\widetilde{q}], M[\widetilde{q}; x]\}$;

(2) $P\|R \approx Q\|R$;

(3) $P[f] \approx Q[f]$;

(4) $P\backslash L \approx Q\backslash L$;

*(5) **if** b **then** $P \approx$ **if** b **then** Q.*

Proof. The proof for (1) is similar to Theorem 38 of [5], and (2)-(5) are direct from Theorem 4.18. □

4.3 Congruent equivalence of quantum processes

As in classical process algebra, the bisimilarity $\approx$ is not preserved by summation combinator "$+$". To deal with this problem, we introduce the notion of equality between quantum processes based on $\approx$.

Definition 4.20 *Two configurations $\langle P, \rho\rangle$ and $\langle Q, \sigma\rangle$ are said to be equal, denoted by $\langle P, \rho\rangle \simeq \langle Q, \sigma\rangle$, if $qv(P) = qv(Q)$, $\mathrm{tr}_{qv(P)}(\rho) = \mathrm{tr}_{qv(Q)}(\sigma)$, and*

(1) whenever $\langle P, \rho\rangle \xrightarrow{\mathsf{c}?q} \mu$, then $\langle Q, \sigma\rangle \Longrightarrow\xrightarrow{\mathsf{c}?q} \nu$ for some ν such that for any super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{qv(\mu)-\{q\}}}$, $\mathcal{E}(\mu) \approx \mathcal{E}(\nu)$;

(2) whenever $\langle P, \rho\rangle \xrightarrow{\alpha} \mu$ where α is not a quantum input, then there exists ν such that $\langle Q, \sigma\rangle \stackrel{\alpha}{\Longrightarrow} \nu$ and $\mu \approx \nu$;

and the symmetric conditions of (1) and (2).

The only difference between the definitions of $\approx$ and $\simeq$ is that in the latter the $\stackrel{\widehat{\alpha}}{\Longrightarrow}$ transition in Clause (2) is replaced by $\stackrel{\alpha}{\Longrightarrow}$; that is, the matching action for a τ-move has to be at least one τ-move.

Furthermore, we lift the definition of equality to quantum processes as follows. For $P, Q \in qProc$, $P \simeq Q$ if and only if for any quantum state $\rho \in \mathcal{D}(\mathcal{H})$ and any indexed set $\widetilde{v}$ of classical values, $\langle P\{\widetilde{v}/\widetilde{x}\}, \rho\rangle \simeq \langle Q\{\widetilde{v}/\widetilde{x}\}, \rho\rangle$ where $\widetilde{x} = fv(P) \cup fv(Q)$.

It is worth noting that all the bisimulation relations proved in the examples of previous subsections are also valid when $\approx$ is replaced by $\simeq$.

Now we prove that the equality relation is preserved by various process constructors of qCCS.

Theorem 4.21 *If $P \simeq Q$ then*

(1) $a.P \simeq a.Q$, $a \in \{\tau, c?x, c!e, \mathsf{c}?q, \mathsf{c}!q, \mathcal{E}[\widetilde{q}], M[\widetilde{q}; x]\}$;

(2) $P + R \simeq Q + R$;

(3) $P \| R \simeq Q \| R$;

(4) $P[f] \simeq Q[f]$;

(5) $P \backslash L \simeq Q \backslash L$;

(6) **if** b **then** $P \simeq$ **if** b **then** Q.

Proof. Similar to the result for bisimulation. □

The monoid laws and the static laws in classical CCS can also be generalized to qCCS.

Theorem 4.22 *For any $P, Q, R \in qProc$, $K, L \subseteq Chan$, any relabeling functions f, f', and any action prefix a, we have*

(1) $P +$ **nil** *$\simeq P$;*

(2) $P + P \simeq P$;

(3) $P + Q \simeq Q + P$;

(4) $P + (Q + R) \simeq (P + Q) + R$;

(5) $P\|\mathbf{nil} \simeq P$;

(6) $P\|Q \simeq Q\|P$;

(7) $P\|(Q\|R) \simeq (P\|Q)\|R$;

(8) $(a.P)\backslash L \simeq \begin{cases} \mathbf{nil}, & \text{if } cn(a) \in L \\ a.P\backslash L, & \text{otherwise} \end{cases}$

(9) $(a.P)[f] \simeq f(a).P[f]$;

(10) $(P+Q)\backslash L \simeq P\backslash L + Q\backslash L$;

(11) $(P+Q)[f] \simeq P[f] + Q[f]$;

(12) $P\backslash L \simeq P$ *if* $cn(P) \cap L = \emptyset$, *where* $cn(P)$ *is the set of free channel names used in* P;

(13) $(P\backslash K)\backslash L \simeq P\backslash(K \cup L)$;

(14) $(P\|Q)\backslash L \simeq P\backslash L\|Q\backslash L$, *if* $cn(P) \cap cn(Q) \cap L = \emptyset$;

(15) $P[f]\backslash L \simeq P\backslash f^{-1}(L)[f]$;

(16) $P[Id] \simeq P$ *where* Id *is the identity relabeling function;*

(17) $P[f] \simeq P[f']$ *if the restrictions of* f *and* f' *on* $cn(P)$ *coincide;*

(18) $P[f][f'] \simeq P[f' \circ f]$;

(19) $(P\|Q)[f] \simeq P[f]\|Q[f]$ *if the restriction of* f *on* $cn(P) \cup cn(Q)$ *is one-to-one.*

Proof. Routine. □

In the following theorem, we simply write $P \xrightarrow{\alpha} P'$ if for any $\rho \in \mathcal{D}(\mathcal{H})$, $\langle P, \rho\rangle \xrightarrow{\alpha} \langle P', \rho\rangle$.

Theorem 4.23 *(Expansion Law) Let*

$$P = (P_1[f_1]\| \cdots \|P_n[f_n])\backslash L.$$

Then

$$\begin{aligned} P \quad \simeq \quad & \sum \left\{ f_i(\alpha).(P_1[f_1]\| \cdots \|P_i'[f_i]\| \cdots \|P_n[f_n])\backslash L : P_i \xrightarrow{\alpha} P_i' \text{ and } f_i(cn(\alpha)) \notin L \right\} \\ + \quad & \sum \left\{ f_i(c?x).(P_1[f_1]\| \cdots \|P_i'[f_i]\| \cdots \|P_n[f_n])\backslash L : P_i \xrightarrow{c?v} P_i'\{v/x\} \text{ for any } v, \text{ and } f_i(c) \notin L \right\} \\ + \quad & \sum \left\{ \mathcal{E}[\widetilde{q}].(P_1[f_1]\| \cdots \|P_i'[f_i]\| \cdots \|P_n[f_n])\backslash L : \langle P_i, \rho\rangle \xrightarrow{\tau} \langle P_i', \mathcal{E}_{\widetilde{q}}(\rho)\rangle \text{ for any } \rho \right\} \\ + \quad & \sum \Bigg\{ M[\widetilde{q}; x].(P_1[f_1]\| \cdots \|P_i'[f_i]\| \cdots \|P_n[f_n])\backslash L : M = \sum_{j \in J} \lambda_j K_j \text{ and} \\ & \qquad \langle P_i, \rho\rangle \xrightarrow{\tau} \boxplus_{j \in J} p_j \bullet \langle P_i'\{\lambda_j/x\}, K_{j,\widetilde{q}} \rho K_{j,\widetilde{q}}/p_j\rangle \text{ for any } \rho \Bigg\} \\ + \quad & \sum \{ \tau.(P_1[f_1]\| \cdots \|P_i'[f_i]\| \cdots \|P_j'[f_j]\| \cdots \|P_n[f_n])\backslash L : \\ & \qquad P_i \xrightarrow{\alpha} P_i', P_j \xrightarrow{\beta} P_j', i < j, f_i(cn(\alpha)) = f_j(cn(\beta)), \text{and} \\ & \qquad \text{among } \alpha \text{ and } \beta \text{ there is exactly one input and one output} \}. \end{aligned}$$

Proof. Routine. □

We now turn to examine the properties of the congruent equivalence $\simeq$ under recursive definitions. To this end, we assume a set of process variable schemes, ranged over by $X, Y, \ldots$. Assigned to each process variable scheme X there is a non-negative integer $ar(X)$. If $\widetilde{q}$ is an indexed set of distinct quantum variables with $|\widetilde{q}| = ar(A)$, then $X(\widetilde{q})$ is called a process variable.

Process expressions may be defined by adding the following clause into Definition 3.1 (and replacing the word "process" by the phrase "process expression" and "qProc" by "qExp"):

(15) $X(\widetilde{q}) \in qExp$, and $qv(X(\widetilde{q})) = \widetilde{q}$

where $X(\widetilde{q})$ is a process variable. We use metavariables $E, F, \ldots$ to range over process expressions. Suppose that E is a process expression, and $\{X_i(\widetilde{q_i}) : i \in I\}$ is a family of process variables. If $\{P_i : i \in I\}$ is a family of processes such that $qv(P_i) \subseteq \widetilde{q_i}$ for all i, then we write

$$E\{P_i/X_i(\widetilde{q_i}) : i \in I\}$$

for the process obtained by replacing simultaneously $X_i(\widetilde{q_i})$ in E with P_i for all $i \in I$.

Definition 4.24 *Let E and F be process expressions containing at most process variables $\{X_i(\widetilde{q_i}) : i \in I\}$. Then E and F are equal, denoted by $E \simeq F$, if for all family $\{P_i : i \in I\}$ of quantum processes with $qv(P_i) \subseteq \widetilde{q_i}$, we have*

$$E\{P_i/X_i(\widetilde{q_i}) : i \in I\} \simeq F\{P_i/X_i(\widetilde{q_i}) : i \in I\}.$$

For simplicity, sometimes we denote $E\{P_i/X_i(\widetilde{q_i}) : i \in I\}$ as $E\{\widetilde{P}/\widetilde{X}\}$ or even $E(\widetilde{P})$ when it does not cause any confusion. The next theorem shows that $\simeq$ is also preserved by recursive definitions.

Theorem 4.25 *(1) If $A(\widetilde{q}) \stackrel{def}{=} P$, then $A(\widetilde{q}) \simeq P$;*

(2) Let $\{E_i : i \in I\}$ and $\{F_i : i \in I\}$ be two families of process expressions containing at most process variables $\{X_i(\widetilde{q_i}) : i \in I\}$, and $E_i \simeq F_i$ for each $i \in I$. If $\{A_i(\widetilde{q_i}) : i \in I\}$ and $\{B_i(\widetilde{q_i}) : i \in I\}$ be two families of process constants such that

$$\begin{aligned} A_i(\widetilde{q_i}) &\stackrel{def}{=} E_i\{A_j(\widetilde{q_j})/X_j(\widetilde{q_j}) : j \in I\} \\ B_i(\widetilde{q_i}) &\stackrel{def}{=} F_i\{B_j(\widetilde{q_j})/X_j(\widetilde{q_j}) : j \in I\}, \end{aligned}$$

then $A_i(\widetilde{q_i}) \simeq B_i(\widetilde{q_i})$ for all $i \in I$.

Proof. (1) is obvious. For (2), we only prove the special case where $|I| = 1$ and for any $i \in I$, $\widetilde{q_i} = \emptyset$. That is, we prove $A \simeq B$ assuming that $qv(A) = qv(B) = \emptyset$, $A \stackrel{def}{=} E(A)$ and $B \stackrel{def}{=} F(B)$ where E and F are process expressions containing process variable X with $qv(X) = \emptyset$, and $E \simeq F$.

Let

$$\mathcal{R} = \{(\langle G(A), \rho\rangle, \langle G(B), \rho\rangle) : \rho \in \mathcal{D}(\mathcal{H}), G \text{ contains at most process variable } X\}.$$

Obviously, for any $\langle G(A), \rho\rangle \mathcal{R} \langle G(B), \rho\rangle$, we have $qv(G(A)) = qv(G(B))$ and $\mathrm{tr}_{qv(G(A))}(\rho) = \mathrm{tr}_{qv(G(B))}(\rho)$. Similar to Propositions 4.12 and 7.8 of [14], we can prove the following properties by induction on the depth of the inference by which the action $\langle G(A), \rho\rangle \stackrel{\alpha}{\longrightarrow} \mu$ is inferred:

(i) whenever $\langle G(A), \rho\rangle \stackrel{c?q}{\longrightarrow} \mu$, then $\langle G(B), \rho\rangle \Longrightarrow\stackrel{c?q}{\longrightarrow} \nu$ such that for any super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{qv(\mu)-\{q\}}}$, $\mathcal{E}(\mu)\mathcal{R}\circ \approx \mathcal{E}(\nu)$;

(ii) whenever $\langle G(A), \rho\rangle \stackrel{\alpha}{\longrightarrow} \mu$ where α is not a quantum input, there exists ν such that $\langle G(B), \rho\rangle \stackrel{\alpha}{\Longrightarrow} \nu$ and $\mu\mathcal{R}\circ \approx \nu$.

Only one case deserves elaboration: when $G = G_1 \| G_2$ and $\langle G(A), \rho \rangle \xrightarrow{\tau} \langle P', \rho \rangle$ is caused by

$$\langle G_1(A), \rho \rangle \xrightarrow{c?q} \langle P'_1, \rho \rangle \quad \text{and} \quad \langle G_2(A), \rho \rangle \xrightarrow{c!q} \langle P'_2, \rho \rangle$$

where $P' = P'_1 \| P'_2$. By induction, we have

$$\langle G_1(B), \rho \rangle \Longrightarrow\xrightarrow{c?q} \boxplus_{i \in I} p_i \bullet \langle Q^i_1, \mathcal{F}'_i(\rho) \rangle$$

where $\mathcal{F}'_i$ is a super-operator acting on $qv(G_1)$ (here Lemma 4.3(2) is used for the $\Longrightarrow$ transition), and for any super-operator $\mathcal{E}$ on $\mathcal{H}_{\overline{qv(P'_1) - \{q\}}}$ and any $i \in I$, it holds

$$\langle P'_1, \mathcal{E}(\rho) \rangle \mathcal{R} \langle Q'_1, \mathcal{E}(\rho) \rangle \approx \langle Q^i_1, \mathcal{E}(\mathcal{F}'_i(\rho)) \rangle. \tag{7}$$

Thus $P'_1 = H_1(A)$ and $Q'_1 = H_1(B)$ for some H_1 containing only process variable X.

Also by induction, we have

$$\langle G_2(B), \rho \rangle \stackrel{c!q}{\Longrightarrow} \boxplus_{j \in J} q_j \bullet \langle Q^j_2, \mathcal{F}_j(\rho) \rangle$$

where $\mathcal{F}_j$ is a super-operator acting on $qv(G_2)$, and for any $j \in J$,

$$\langle P'_2, \rho \rangle \mathcal{R} \langle Q'_2, \rho \rangle \approx \langle Q^j_2, \mathcal{F}_j(\rho) \rangle. \tag{8}$$

Thus $P'_2 = H_2(A)$ and $Q'_2 = H_2(B)$ for some H_2 containing only process variable X.

Now by inference rule **Q-Com**, and noting that $\mathcal{F}'_i$ and $\mathcal{F}_j$ commute for any $i \in I$ and $j \in J$ since $qv(G_1) \cap qv(G_2) = \emptyset$, we derive that

$$\langle G(B), \rho \rangle \stackrel{\tau}{\Longrightarrow} \boxplus_{i \in I} \boxplus_{j \in J} p_i q_j \bullet \langle Q^i_1 \| Q^j_2, \mathcal{F}_j(\mathcal{F}'_i(\rho)) \rangle.$$

Now we calculate that for any $i \in I$ and $j \in J$,

$$\begin{array}{rcll}
\langle P'_1 \| P'_2, \rho \rangle & = & \langle (H_1 \| H_2)(A), \rho \rangle & \\
& \mathcal{R} & \langle (H_1 \| H_2)(B), \rho \rangle & \text{By definition} \\
& = & \langle Q'_1 \| Q'_2, \rho \rangle & \\
& \approx & \langle Q'_1 \| Q^j_2, \mathcal{F}_j(\rho) \rangle & \text{By Eq.(8) and Theorem 4.18} \\
& \approx & \langle Q^i_1 \| Q^j_2, \mathcal{F}_j(\mathcal{F}'_i(\rho)) \rangle & \text{By Eq.(7), Lemma 3.2, and Theorem 4.18.}
\end{array}$$

Similarly, we can prove the symmetric form of (i) and (ii) for $\langle G(B), \rho \rangle \xrightarrow{\alpha}$. Then $\mathcal{R}$ is a bisimulation up to $\approx$, and so $\mathcal{R} \subseteq \approx$ by Lemma 4.17. Now from (i) and (ii) again, we have $\langle G(A), \rho \rangle \simeq \langle G(B), \rho \rangle$. Taking $G = X$ and noting the arbitrariness of ρ, we have $A \simeq B$. $\square$

Finally, the uniqueness of solutions of equations can be proved for process expressions in qCCS.

Definition 4.26 *Given a process variable $X(\widetilde{q})$ and a process expression E, we call*

- *$X(\widetilde{q})$ is sequential in E if every subexpression of E which contains $X(\widetilde{q})$, excluding $X(\widetilde{q})$ itself, is of the form $a.F$, $\sum_{i \in I} F_i$, or* **if** *b* **then** *F;*
- *$X(\widetilde{q})$ is guarded in E if each occurrence of $X(\widetilde{q})$ is within some subexpression $a.F$ of E where a is a (classical or quantum) input or output.*

We also say that E is sequential (resp. guarded) if each process variable is sequential (resp. guarded) in E.

Lemma 4.27 *Let G be guarded and sequential, and contain at most process variables $\widetilde{X}$. If $\langle G(\widetilde{P}), \rho\rangle \xrightarrow{\alpha} \boxplus_{i\in I} p_i \bullet \langle P_i', \rho_i\rangle$. Then there exist sequential process expressions $\{H_i : i \in I\}$, containing at most process variables $\widetilde{X}$, such that $P_i' = H_i(\widetilde{P}_\alpha)$ for each i, and for any $\widetilde{Q}$, $\langle G(\widetilde{Q}), \rho\rangle \xrightarrow{\alpha} \boxplus_{i\in I} p_i \bullet \langle H_i(\widetilde{Q}_\alpha), \rho_i\rangle$. Here*

$$\widetilde{P}_\alpha = \begin{cases} \widetilde{P}\{r/q\} \text{ for some } q \in qv(\widetilde{P}), & \text{if } \alpha = \mathsf{c}?r \\ \widetilde{P}\{v/x\} \text{ for some } x \in fv(\widetilde{P}), & \text{if } \alpha = c?v \text{ or } \alpha = \tau \text{ is caused by a measurement} \\ \widetilde{P}, & \text{otherwise} \end{cases}$$

and $\widetilde{Q}_\alpha$ is defined similarly. Moreover, if $\alpha = \tau$, then H_i is guarded.

Proof. Similar to Lemma 7.12 of [14]. □

Theorem 4.28 *Let $\{E_i : i \in I\}$ be a family of process expressions containing at most process variables $\{X_i(\widetilde{q_i}) : i \in I\}$, and each $X_j(\widetilde{q_j})$ is sequential and guarded in each E_i. Let $\{P_i : i \in I\}$ and $\{Q_i : i \in I\}$ be two families of quantum processes such that $qv(P_i) \cup qv(Q_i) \subseteq \widetilde{q_i}$ for each i, and*

$$\begin{aligned} P_i &\simeq E_i\{P_j/X_j(\widetilde{q_j}) : j \in I\} \\ Q_i &\simeq E_i\{Q_j/X_j(\widetilde{q_j}) : j \in I\}, \end{aligned}$$

then $P_i \simeq Q_i$ for all $i \in I$.

Proof. For simplicity, we only prove the case where $|I| = 1$ and all the processes contain no free classical or quantum variables. That is, we prove $P \simeq Q$ assuming that $qv(P) = qv(Q) = \emptyset$, $fv(P) = fv(Q) = \emptyset$, $P \simeq E(P)$, and $Q \simeq E(Q)$, where E contains at most process variable X.

Let

$$\begin{aligned} \mathcal{R} \;=\; \{(\langle M,\rho\rangle, \langle N,\sigma\rangle) : \langle M,\rho\rangle \approx \langle H(P),\eta\rangle \text{ and } \langle N,\sigma\rangle \approx \langle H(Q),\eta\rangle, \\ \text{for some } \eta \in \mathcal{D}(\mathcal{H}), H \text{ is sequential and contains at most } X\}. \end{aligned}$$

We show $\mathcal{R}$ is a bisimulation. The proof is somewhat similar to Proposition 7.13 in [14]. We first claim that for any $\langle M,\rho\rangle \mathcal{R} \langle N,\sigma\rangle$,

$$\text{If } \langle M,\rho\rangle \Longrightarrow \mu, \text{ then } \langle N,\sigma\rangle \Longrightarrow \nu \text{ such that } \mu\mathcal{R}\nu \tag{9}$$

Suppose $\langle M,\rho\rangle \Longrightarrow \mu$. Then $\langle H(P),\eta\rangle \Longrightarrow \mu_1$, $\mu \approx \mu_1$, from $\langle M,\rho\rangle \approx \langle H(P),\eta\rangle$. By Theorem 4.21, we have $H(E(P)) \simeq H(P)$, so $\langle H(E(P)),\eta\rangle \Longrightarrow \mu_2$ such that $\mu_1 \approx \mu_2$. Note that X is both sequential and guarded in $H(E(P))$. By repeatedly using Lemma 4.27, we have $\mu_2 = \boxplus_{i\in K} p_i \bullet \langle H_i'(P), \rho_i\rangle$, and

$$\langle H(E(Q)),\eta\rangle \Longrightarrow \nu_2 = \boxplus_{i\in K} p_i \bullet \langle H_i'(Q), \rho_i\rangle$$

where H_i' is sequential for any $i \in K$. Since $H(E(Q)) \simeq H(Q)$ and $\langle N,\sigma\rangle \approx \langle H(Q),\eta\rangle$, we have $\langle H(Q),\eta\rangle \Longrightarrow \nu_1$, $\nu_2 \approx \nu_1$, and $\langle N,\sigma\rangle \Longrightarrow \nu$, $\nu_1 \approx \nu$. Furthermore, it is obvious that $\mu_2\mathcal{R}\nu_2$ from Lemma 4.6, and then $\mu\mathcal{R}\nu$ by Lemma 4.5 since $\approx \circ \mathcal{R} \circ \approx \subseteq \mathcal{R}$.

Now let $\langle M,\rho\rangle \xrightarrow{\alpha} \mu$ where $\alpha \neq \tau$. There are two cases:

(1) $\alpha = \mathsf{c}?q$ is a quantum input. Then $\mu = \langle M',\rho\rangle$ for some M'. So $\langle H(P),\eta\rangle \overset{\mathsf{c}?q}{\Longrightarrow} \mu_1$ such that $\mathcal{E}(\mu) \approx \mathcal{E}(\mu_1)$ for any super-operator $\mathcal{E}$ acting on $\mathcal{H}_{\overline{qv(\mu)-\{q\}}}$. By Theorem 4.12 we further have $\langle H(E(P)),\eta\rangle \overset{\mathsf{c}?q}{\Longrightarrow} \mu_2$ such that $\mathcal{F}(\mu_1) \approx \mathcal{F}(\mu_2)$ for any super-operator $\mathcal{F}$ acting on $\mathcal{H}_{\overline{qv(\mu_1)-\{q\}}}$. Note that X is both sequential and guarded in $H(E(P))$. By repeatedly using Lemma 4.27, we have $\mu_2 = \boxplus_{j\in J} q_j \bullet \langle H_j'(P), \rho_j'\rangle$, and

$$\langle H(E(Q)),\eta\rangle \overset{\mathsf{c}?q}{\Longrightarrow} \nu_2 = \boxplus_{j\in J} q_j \bullet \langle H_j'(Q), \rho_j'\rangle$$

where H'_j is sequential for any $j \in J$. Using Theorem 4.12 again we have $\langle H(Q), \eta\rangle \Longrightarrow\xrightarrow{\mathsf{c}?q} \nu_1$ such that $\mathcal{F}'(\nu_2) \approx \mathcal{F}'(\nu_1)$ for any super-operator $\mathcal{F}'$ acting on $\mathcal{H}_{\overline{qv(\nu_2)-\{q\}}}$, and $\langle N, \sigma\rangle \Longrightarrow\xrightarrow{\mathsf{c}?q} \nu$ such that $\mathcal{E}'(\nu_1) \approx \mathcal{E}'(\nu)$ for any super-operator $\mathcal{E}'$ acting on $\mathcal{H}_{\overline{qv(\nu_1)-\{q\}}}$. Finally, since $qv(\mu) = qv(\mu_1) = qv(\nu_i)$, we have

$$\mathcal{G}(\mu) \approx \mathcal{G}(\mu_1) \approx \mathcal{G}(\mu_2) \text{ and } \mathcal{G}(\nu_2) \approx \mathcal{G}(\nu_1) \approx \mathcal{G}(\nu)$$

for any super-operator $\mathcal{G}$ acting on $\mathcal{H}_{\overline{qv(\mu)-\{q\}}}$. Note that by Lemma 4.6, $\mathcal{G}(\mu_2)\mathcal{R}\mathcal{G}(\nu_2)$. Then $\mathcal{G}(\mu_2)\mathcal{R}\mathcal{G}(\nu_2)$ from Lemma 4.5 since $\approx\circ\mathcal{R}\circ\approx\subseteq\mathcal{R}$.

(2) α is a quantum output or classical input/output. Then $\langle H(P), \eta\rangle \stackrel{\alpha}{\Longrightarrow} \mu_1$, $\mu \approx \mu_1$, and $\langle H(E(P)), \eta\rangle \stackrel{\alpha}{\Longrightarrow} \mu_2$, $\mu_1 \approx \mu_2$. We further break the sequence of actions of $\langle H(E(P)), \eta\rangle$ into

$$\langle H(E(P)), \eta\rangle \Longrightarrow\xrightarrow{\alpha} \mu_3 \Longrightarrow \mu_2.$$

Note that X is both sequential and guarded in $H(E(P))$. By repeatedly using Lemma 4.27, we have $\mu_3 = \boxplus_{i\in K} p_i \bullet \langle H'_i(P), \rho_i\rangle$, and

$$\langle H(E(Q)), \eta\rangle \Longrightarrow\xrightarrow{\alpha} \nu_3 = \boxplus_{i\in K} p_i \bullet \langle H'_i(Q), \rho_i\rangle$$

where H'_i is sequential. For any $i \in K$, it is obvious that $\langle H'_i(P), \rho_i\rangle\mathcal{R}\langle H'_i(Q), \rho_i\rangle$. So by Eq.(9) we have $\nu_3 \Longrightarrow \nu_2$ such that $\mu_2\mathcal{R}\nu_2$. We further derive $\langle H(Q), \eta\rangle \stackrel{\alpha}{\Longrightarrow} \nu_1$, $\nu_2 \approx \nu_1$ and $\langle N, \sigma\rangle \stackrel{\alpha}{\Longrightarrow} \nu$, $\nu_1 \approx \nu$. Finally, we have $\mu\mathcal{R}\nu$ from $\mu_2\mathcal{R}\nu_2$.

We have proved that $\mathcal{R}$ is a bisimulation. In particular, for any sequential H, $H(P) \approx H(Q)$. Since E is guarded and sequential, every occurrence of X is within some subexpression $a.F$ of E where F is also sequential. Then we have $F(P) \approx F(Q)$, and then $a.F(P) \simeq a.F(Q)$. Thus $E(P) \simeq E(Q)$ by Theorem 4.21. Now the result $P \simeq Q$ follows from $P \simeq E(P)$ and $Q \simeq E(Q)$. □

To illustrate the power of the theorems proved in this section, let us reconsider Example 4.11. We will provide another proof for $\mathcal{U}(U) \circ \mathcal{U}(V) \simeq \mathcal{U}(VU)$ using the Expansion law and the uniqueness of solutions of equations. For simplicity, we only consider the special case where U and V are both 1-qubit unitary operators. Recall the definition of $\mathcal{U}(U) \circ \mathcal{U}(V)$ in Example 3.6:

$$\mathcal{U}(U) \circ \mathcal{U}(V) \quad \stackrel{def}{=} \quad (L_s \| \mathcal{U}(U)[\mathsf{e}/\mathsf{c}, \mathsf{f}/\mathsf{d}] \| \mathcal{U}(V)[\mathsf{f}/\mathsf{c}, \mathsf{g}/\mathsf{d}] \| R_s)\backslash L$$

where $L = \{c, \mathsf{e}, \mathsf{f}, \mathsf{g}\}$. Then from Theorem 4.25(1), and repeatedly using Theorems 4.23 and 4.21, we have

$$\mathcal{U}(U) \circ \mathcal{U}(V) \quad \simeq \quad \mathsf{c}?q.\tau.U[q].\tau.V[q].\tau.\mathsf{d}!q.\tau.\mathcal{U}(U) \circ \mathcal{U}(V)$$

where the first τ action is caused by interaction between L_s and $\mathcal{U}(U)[\mathsf{e}/\mathsf{c}, \mathsf{f}/\mathsf{d}]$, the second one between $\mathcal{U}(U)[\mathsf{e}/\mathsf{c}, \mathsf{f}/\mathsf{d}]$ and $\mathcal{U}(V)[\mathsf{f}/\mathsf{c}, \mathsf{g}/\mathsf{d}]$, the third one between $\mathcal{U}(V)[\mathsf{f}/\mathsf{c}, \mathsf{g}/\mathsf{d}]$ and R_s, while the last one between R_s and L_s.

On the other hand, by Theorem 4.25(1) we have

$$\mathcal{U}(VU) \quad \simeq \quad \mathsf{c}?q.VU[q].\mathsf{d}!q.\mathcal{U}(VU).$$

Now let X be a quantum process variable with $qv(X) = \emptyset$, and

$$E = \mathsf{c}?q.\tau.U[q].\tau.V[q].\tau.\mathsf{d}!q.\tau.X, \qquad F = \mathsf{c}?q.VU[q].\mathsf{d}!q.X$$

be two quantum process expressions. Then E and F are both sequential and guarded, and $E \simeq F$. So we have $\mathcal{U}(U) \circ \mathcal{U}(V) \simeq \mathcal{U}(VU)$ from Theorem 4.28.

5 Conclusions and further work

In this paper, we propose a formal model qCCS, which is a quantum extension of classical value-passing CCS, to model and rigorously analyze the behaviors of quantum distributed computing and quantum communication protocols. We define a notion of equivalence, based on bisimulation, for quantum processes in qCCS, and prove that it is preserved by all process constructors, including parallel composition, restriction, and recursive definitions. This is the first congruent equivalence for process algebras proposed so far aiming at modeling quantum communicating systems. Various examples are fully examined to show the expressiveness as well as the proof techniques of qCCS.

We conclude this paper by pointing out some topics for further study. In the present paper, only *exact* bisimulation is presented where two quantum processes are either bisimilar or non-bisimilar. Obviously, such a bisimulation cannot capture the idea that a quantum process *approximately* implements its specification. Note that this approximation, or imprecision, is especially essential for quantum process algebra since quantum operations constitute a continuum and exact bisimulation is not always practically suitable for their physical implementation. To provide techniques and tools for approximate reasoning, a quantified version of bisimulation, which defines for each pair of quantum processes a bisimulation-based distance characterizing the extent to which they are bisimilar, has already been proposed for purely quantum processes in [19]. We plan to extend it to qCCS defined in this paper.

Another interesting direction worthy of being researched is to expand the application scope of qCCS to model and analyze the *security properties* of quantum cryptographic systems. By introducing cryptographic primitives, such as constructors for encryption and decryption, into pi-calculus, the Spi calculus [1] has been very successful in cryptographic protocol analysis. We believe that a similar extension of our qCCS will provide tools for analyzing quantum cryptographic protocols such as BB84 quantum key distribution protocol.

Acknowledgement

The authors thank the colleagues in the Quantum Computation and Quantum Information Research Group for useful discussion. This work was partially supported by the FANEDD under Grant No. 200755 and the Natural Science Foundation of China (Grant Nos. 60503001 and 60621062).

References

[1] M Abadi and AD Gordon. A calculus for cryptographic protocols: the spi calculus, 1997.

[2] Christel Baier and Marta Kwiatkowska. Domain equations for probabilistic processes. *Mathematical Structure in Computer Science*, 1999.

[3] C. H. Bennett, G. Brassard, C. Crepeau, R. Jozsa, A. Peres, and W. Wootters. Teleporting an unknown quantum state via dual classical and epr channels. *Physical Review Letters*, 70:1895–1899, 1993.

[4] C. H. Bennett and S. J. Wiesner. Communication via one- and two-particle operators on einstein-podolsky-rosen states. *Physical Review Letters*, 69(20):2881–2884, 1992.

[5] Y Feng, R Duan, Z Ji, and M Ying. Probabilistic bisimulations for quantum processes. *Information and Computation*, 205(11):1608–1639, 2007.

[6] S. J. Gay and R. Nagarajan. Communicating quantum processes. In J. Palsberg and M. Abadi, editors, *Proceedings of the 32nd ACM SIGPLAN-SIGACT Symposium on Principles of Programming Languages (POPL)*, pages 145–157, 2005.

[7] L. K. Grover. Quantum mechanics helps in searching for a needle in a haystack. *Physical Review Letters*, 78(2):325, 1997.

[8] M. Hennessy. A proof system for communicating processes with value-passing. *Formal Aspects of Computer Science*, 3:346–366, 1991.

[9] M. Hennessy and A. Ingólfsdóttir. A theory of communicating processes value-passing. *Information and Computation*, 107(2):202–236, 1993.

[10] P. Jorrand and M. Lalire. Toward a quantum process algebra. In P. Selinger, editor, *Proceedings of the 2nd International Workshop on Quantum Programming Languages, 2004*, page 111, 2004.

[11] K. Kraus. *States, Effects and Operations: Fundamental Notions of Quantum Theory*. Springer, Berlin, 1983.

[12] Marie Lalire. Relations among quantum processes: Bisimilarity and congruence. *Mathematical Structures in Computer Science*, 16(3):407–428, 2006.

[13] R. Milner, J. Parrow, and D. Walker. A calculus of mobile processes, parts i and ii. *Information and Computation*, 100:1–77, 1992.

[14] Robin Milner. *Communication and Concurrency*. Prentice Hall, Englewood Cliffs, NJ, 1989.

[15] M. Nielsen and I. Chuang. *Quantum computation and quantum information*. Cambridge university press, 2000.

[16] P. Selinger. Towards a quantum programming language. *Mathematical Structures in Computer Science*, 14(4):527–586, 2004.

[17] P. W. Shor. Algorithms for quantum computation: discrete log and factoring. In *Proceedings of the 35th IEEE FOCS*, pages 124–134, 1994.

[18] J. von Neumann. *Mathematical Foundations of Quantum Mechanics*. Princeton University Press, Princeton, NJ, 1955.

[19] M Ying, Y Feng, R Duan, and Z Ji. An algebra of quantum processes. *ACM Transactions on Computational Logic (TOCL)*, 10(3):1–36, 2009.